"CRIPTOGRAFIA EM SEGURANÇA DE ARQUIVOS CONFIDENCIAIS"

Yatosi Masuda

TESE SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIA (M.Sc.).

Aprovada por:

Presidente

RIO DE JANEIRO

ESTADO DA GUANABARA - BRASIL

SETEMBRO DE 1973

Aos meus pais
Hideki e Tokie
e a minha esposa
Elisa.

AGRADECIMENTOS

- À COPPE pela oportunidade,
- Ao CNPq pela concessão da bolsa de estudos,
- Ao Prof. J. Pierre Lavelle pelo assunto e orientação,
- Ao Prof. Celso Renna e Souza pelos incentivos,
- Ao Dr. G. Estellita Lins, chefe da Assessoria de Pesquisa Operacional (BNH) por conceder horários especiais para frequentar a COPPE,
- À equipe de Administração da APO, chefiada pelo Sr. Oswaldo de Souza pela dedicação nos trabalhos de datilografia, correção e desenhos.
- A todos aqueles que indiretamente contribuiram para a confecção desta Tese.

RESUMO

Este trabalho é um estudo sôbre segurança em Centros de Processamento de Dados e segurança de informações confidenciais.

Muitos fatos que podem surgir e abalar qualquer CPD, tais como: fraudes, falhas de hardware e/ou software, erros do operador, erros de programação, penetração em informações privativas, e outros, são brevemente abordados.

Com referência a segredo de informação, as técnicas clássicas de criptografia são estudadas. Com base nisso, técnicas de transformação adequadas, tais como, esquemas aritméticos, lógicos e esquema de matriz são descritas.

Finalmente é dada uma discussão sobre o projeto de sistemas de cripto-programação.

ABSTRACT

This work is a study about security of Data Processing Center and Security of private informations.

Many destructive fates that can await every Computer Center: fraud, hardware and software failures, operator errors, programming errors, penetration of private informations and others, are briefly discussed.

With reference of privacy of information, the classical criptographic techniques are studied. On this bases, suitable transformation techniques such as arithmetical, logic and matrix schemes are discribed.

Finally a discussion is given on the systems design for criptoprogramming.

ÍNDICE

I. INTRODUÇÃO

O crescente aumento de centros de processamento de dados, bem como a possibilidade de grande número de sistemas multi-terminais "on-line" e de "time-sharing" virem a surgir, tanto na área comercial como nas Universidades, faz pensar na necessidade de se manter um nível de segurança desejável nas informações confidenciais, assim como em todas as instalações de um centro de processamento.

Não nos esqueçamos, também, da área militar, onde tentativas de espionagens para obter segredos de segurança nacional regularmente tem aparecido nos noticiários de várias partes do globo.

Desde que esta área começa a fazer maior uso de sistemas de computadores, seus segredos naturalmente estarão guardados em arquivos computacionais, e uma tentativa deliberada de penetrar nos arquivos deve e pode ser evitada antecipadamente.

Há uma correspondente situação no mundo dos negócios e nas indústrias.

Muitas informações comerciais são privativas das companhias. Algumas dessas informações poderiam dizer respeito à tecnologia desenvolvida na empresa, ou à sua situação financeira.

Em ambos os casos a criptografia poderá ajudar em muito a elevar o custo das infiltrações a um preço alto, de tal forma a desencorajar tais tentativas.

Como os computadores crescem em importância dentro de uma orga

nização, a necessidade de proteção contra sabotagem, incêndio, inundações e fraudes aumenta.

Certas organizações nos E.E.U.U. tem ido à falência depois de constatar irregularidades em seu centro de processamento; outras têm-se levantado com enormes dificuldades.

Procuraremos neste trabalho visualizar algumas ameaças contra o bom andamento de um C P D, e os procedimentos corretivos.

Quanto aos arquivos de dados confidenciais ou transmissões entre computador e terminais, vamos nos ater às técnicas clássicas de criptografia; partindo daí para técnicas mais modernas próprias para sistemas computacionais.

II. CENTRO DE PROCESSAMENTO DE DADOS E SUA SEGURANÇA GERAL

II.1. Os Problemas de Segurança em C P D.

Bem poucas companhias de processamento de dados têm tomado as mais insignificantes precauções para garantir o contínuo funcionamento de suas instalações.

Todo sistema é sensível a acidentes, desastres, e até sabotagem.

Se uma companhia faz um grande investimento no seu sistema, como mais e mais está se fazendo atualmente, pouca segurança significará que estes sistemas constituem um real tendão de Aquiles.

É realmente verdade, hoje em dia, que firmas usando modernas técnicas de processamento de dados têm a maior parte de suas atividades concentradas na sala de computação, onde são realizadas as operações básicas do sistema.

Este fato sugere algumas sérias questões de segurança a considerar:

. Estaria a companhia livre de paralização dos seus negócios se o centro de computação ou algum dos seus componentes sofresse uma repentina destruição?

.. A companhia proporciona a seus arquivos computacionais (fitas, cartões, discos) segurança e proteção comparável com a segurança de outros componentes que não seja o computador?

... Há alguma proteção para os programas, arquivos e equipamento contra sabotagem ?

Em pesquisa feita nos E.E.U.U. em muitas companhias, seus executivos não souberam responder a tais perguntas, de onde se conclui que os riscos são todos eles negligenciados.

As consequências de um sistema com pouca segurança na área de Processamento de Dados pode ser alguns casos, e assim tem sido fatal.

II.2. Ameaças a Segurança de um Centro de Processamento de Dados (Riscos).

Os exemplos que se seguem descrevem as espécies de ameaças à segurança a que um sistema em geral pode estar sujeito, bem como as medidas a serem tomadas.

Desastre Acidental:

Inundações e incêndios são considerados acidentais e causam grandes prejuízos em CPD.

Um acidente típico que se pode citar é o caso acontecido num CP situado no segundo pavimento de um edifício.

Tal andar estava projetado contra incêndio. No entanto, o primeiro pavimento não tinha aquela especificação e quando foi destruído pelas chamas fez ruir todas as instalações do andar superior.

Todo um trabalho de planificação antes da instalação do computador deve ser feito, afim de evitar futuros problemas.

Naturalmente o lado econômico é um fator de elevada ponderação.

O serviço de reparo e manutenção urgentes precisam estar bem equipados.

Assim, se ocorrer uma paralização no sistema elétrico de força, ou o ar condicionado for subitamente interrompido, ou se há uma falha no computador, somente os CPD que possuem aquelas facilidades podem continuar a operar.

Falhas Mecânicas:

Pequenas falhas mecânicas podem causar problemas de grandes dimensões.

Uma descoberta do mau funcionamento de um equipamento elétrico de manuseio de fitas magnéticas depois que se havia processado uma enorme quantidade de "carreteis" fêz daquele trabalho uma verdadeira inutilidade.

Erro do Operador:

O computador pode, às vezes, inadvertidamente, destruir volumosos programas e arquivos de dados.

Isto ocorre se a máquina for impropriamente operada por pessoa inexperiente.

Um caso já acontecido foi o rompimento de uma fita magnética

devido à excessiva velocidade proporcionada pelo operador.

Erros de Programas:

Erros de programação causam imensos contra-tempos.

Quantas vezes verificamos as reformulações em listas de aprovações em exames vestibulares devido a erros de programação.

Houve até o caso de um foguete ter de ser destruído devido ao Erro da programação.

Roubos e Fraudes:

Uma fita com 50 milhões de caracteres de dados pode ser copiada em poucos minutos, não deixando vestígios de tal procedimento. Esta fita poderia conter valiosos programas ou dados pessoais valiosos, ou outra quantidade qualquer de informações importantes.

Sabotagem:

De todas as ameaças, esta talvez seja a que oferece maior perigo.

Considere o exemplo acontecido:

Um funcionário insatisfeito com a firma onde trabalhava destruiu todos os arquivos e programas que a companhia processara, com a ajuda de um ímã.

Reconstruir os dados tomaria muito tempo, pelo menos no parecer do auditor, o qual não estava certo de que poderia reconstruir as informações suficientes para manter a companhia no negócio.

Uma outra ocorrência, esta se bem que involuntária, foi a visita de um grupo de anciãs a um centro de processamento. Uma delas retirou um cartão do meio de um programa, deixado sobre a mesa, como souvenir.

A consequência desse ato é fácil de imaginar: todo um programa sendo rodado inutilmente.

Medidas de Segurança:

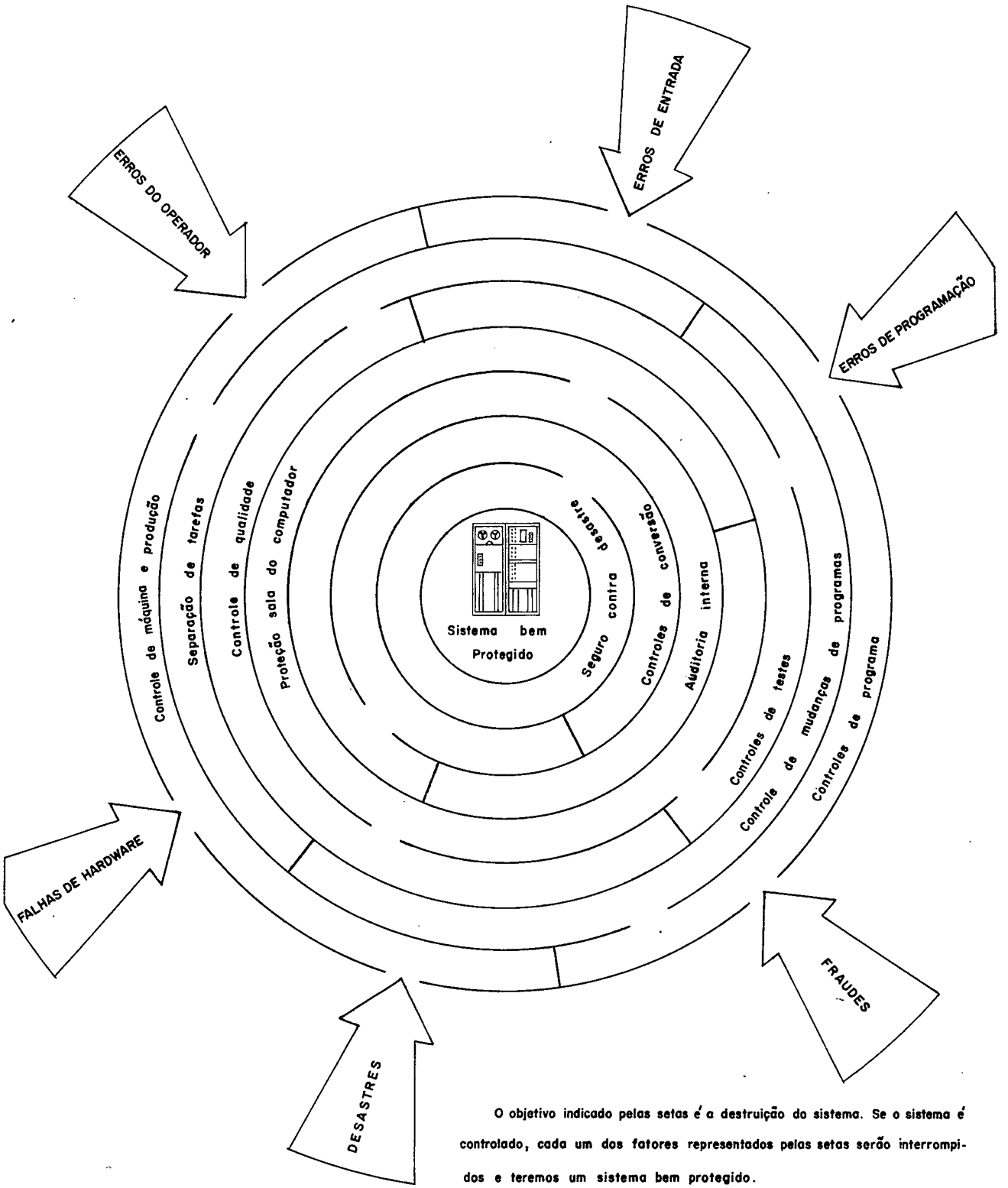
OBJETO	MEDIDA
Acesso	Controlado
Arquivo de Fitas	Duplicação e Guardados em lugar Separado.
Biblioteca de Programas e Dados	Controle de Retiradas
Programa	Controlado por "Chaves" Próprias.
Segurança	Grupo Interno Segurança.

O quadro acima aponta algumas medidas de segurança que podem ser implantadas em um CPD.

Primeiramente, é necessário medir os riscos a que uma companhia está exposta, para em seguida estimar o custo de uma proteção e tomar as ações de segurança apropriadas.

Em suma, devem-se aplicar os mesmos métodos e disciplinas para a segurança do CPD que se aplicam para todas as outras partes da companhia.

Fig. 1 LABIRINTO DE CONTROLE



O objetivo indicado pelas setas é a destruição do sistema. Se o sistema é controlado, cada um dos fatores representados pelas setas serão interrompidos e teremos um sistema bem protegido.

III. SISTEMAS DE PROCESSAMENTO DE DADOS COM INFORMAÇÕES E ARQUIVOS CONFIDENCIAIS: SUA SEGURANÇA

III.1. Identificação do Problema

Com o surgimento de sistemas multi-terminais, "on-line" e de "time-sharing", uma rede, de Bancos de Dados consequentemente será uma realidade.

Acredita-se que tal evento é tão inevitável como as redes telefônica e elétrica que a precederam. É muito menos caro e mais eficiente partilhar informações do que reproduzí-las.

Infelizmente, as redes atuais de informação não possuem garantias adequadas para proteção de informações confidenciais ou secretas.

Dois importantes problemas, segredo e segurança, são tópicos no grande número de discussões sobre o controle de acesso a informações guardadas em arquivos computacionais.

Embora, não haja muita consistência na terminologia usada por vários autores nesse campo, podemos propor, para identificação desses dois problemas, a seguinte maneira:

Segredo de informação - envolve questões de leis, éticas e juízo.

Quando ou não um particular indivíduo teria acesso a uma específica parte das informações é uma questão de segredo de informação.

Segurança de informação - envolve questões de meios, procedimentos para garantir que as decisões de segredo sejam de fato executáveis e aplicáveis.

A tabela abaixo mostra as consequências de cada possível combinação de decisão de segredo e ação de segurança.

DECISÃO DE SEGREDO

Tab. 1

Ação do Sistema de Segurança	Acesso Permitido	Acesso Negado
Acesso Obtido	Acesso Natural	Invasão Bem Sucedida
Acesso Impedido	Recusa Imprópria	Defesa Bem Sucedida

III.2. Problemas de Segurança no Sistema de Processamento de Dados

Há vários tipos de ameaças para um sistema que poderiam ser consideradas (Tab. 2).

Um estranho, por exemplo, tentando usar o terminal de um sistema de "time-sharing", sem autorização. Pela observação de outros usuários, aprenderia como usá-lo.

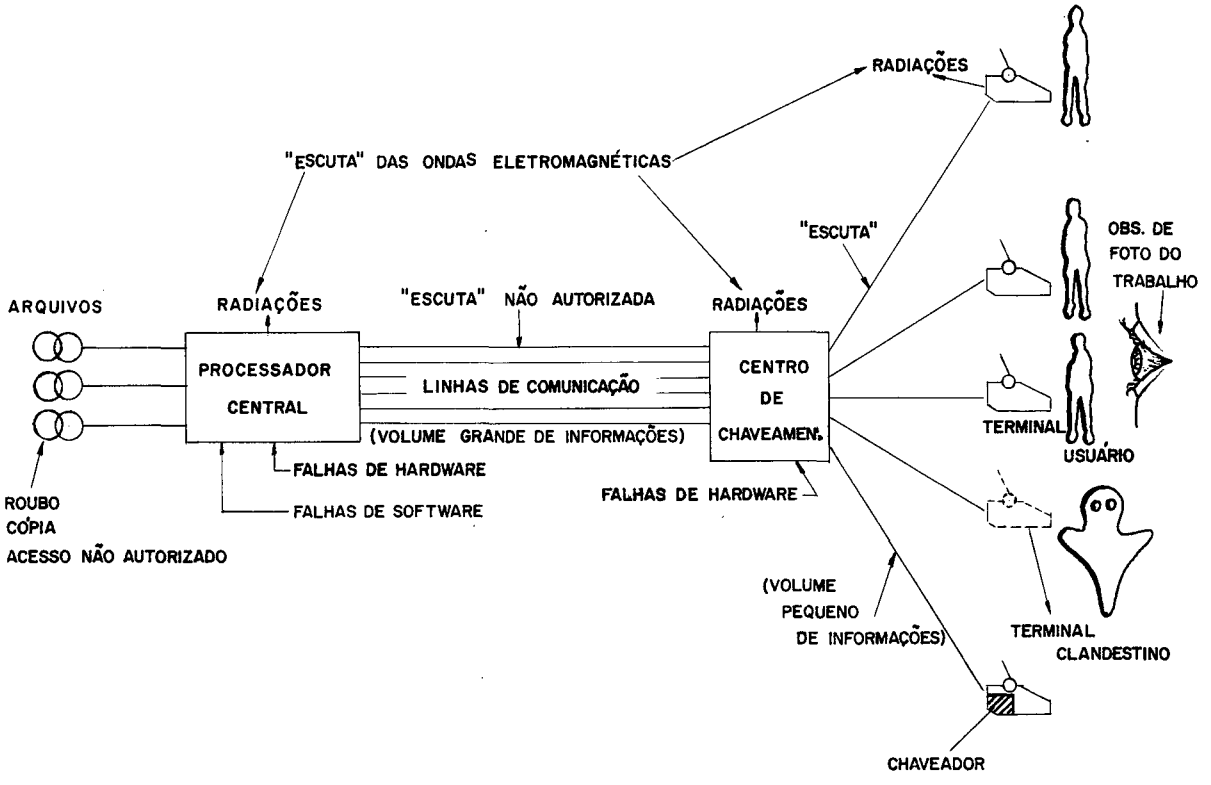
Seu propósito poderia ser o de usar o terminal sem que fosse necessário pagar por isso, ou usar o sistema para obter informações privativas. Uma vez dentro do sistema, poder-se-iam modificar muitas informações de seu interesse.

Outro tipo de problema de segurança é a possibilidade de copiar arquivos. Se um arquivo completo é copiado e entregue a pessoa não autorizada, isso poderá resultar em grandes prejuízos.

A fig. (2) nos mostra um sistema típico de "time-sharing", bem como os problemas e ameaças ao sistema.

Fig.2

Ameaças a um sistema típico de "time-sharing"



Muitos usuários de computadores comerciais não constatam que a transmissão de informação digital não é mais segura do que o código Morse ou a conversação telefônica, desde que a tecnologia necessária para interpretar dados computacionais, é grandemente difundida.

Embora já se tenha aplicado "transformações secretas" entre usuário-processador, só recentemente se teve ciência das ameaças de infiltração.

"Retirar" e "escutar" informações, camufladamente, é classificada como forma de infiltração passiva.

Infiltração ativa pode proporcionar uma ameaça maior.

Algumas das categorias de infiltração ativa incluem:

. Intimidação - uso de acesso legítimo do sistema para obter informações não autorizadas.

. Falsificação - fazer-se de um legítimo usuário, após obter identificação própria, por meios ilegais.

. Entrada-"entre-linhas" - penetração no sistema quando o usuário legítimo está em um canal, mas seu terminal está inativo.

. Entrada ilegal - interpretação seletiva da comunicação usuário-processa

dor e o retorno de uma falsa mensagem ao usuário.

. Descarga de memória para obtenção de informação residual.

Algumas vezes um usuário pode inadvertidamente ganhar acesso a algum arquivo de outro. Uma linha telefônica com ruídos, por exemplo, pode causar uma "caída" na ligação, isto é, o ruído força os dados a colocarem-se dentro da condição de "fora do gancho". Se a identificação do usuário já foi feita, a próxima pessoa a usar a linha telefônica para entrar em contacto com o computador poderá receber os dados do primeiro usuário.

Um meio de evitar a vulnerabilidade das linhas de comunicação de dados é por meio da "criptagem" do sinal a ser transmitido, por meio de uma aparelhagem adequada ou codificando-se a mensagem usando esquemas tradicionais de criptografia.

A essas mudanças na mensagem chamamos de transformações secretas ou de segurança.

Tab.2

ALGUMAS AMEAÇAS À SEGURANÇA DE INFORMAÇÃO

Acidental
erro do usuário
erro do sistema
Deliberado, passivo
métodos eletromagnéticos
escuta com gravador em linha telefônica
Deliberado ativo
intimidação
passar-se por outro usuário
entrada "entre-linhas" enquanto o usuário está inativo, porém no canal.
infiltração externa através de interceptação e de transmissão de uma mensagem de erro ao usuário.
descarga de memória

III.3. Transformações Secretas (ou de segurança)

As transformações de segurança são codificações reversíveis usadas para ocultar a informação. São úteis para proteção contra gravação de dados em linhas telefônicas, em fita magnética, tratamento de radiações eletromagnéticas de terminais, infiltração externa e acesso não autorizado a dados em arquivos removíveis. (ver fig.2).

A substituição (de um caráter na cadeia por um outro), a transposição (remanejamento da ordenação de caracteres em uma mensagem) e a adição (combinando algebricamente caracteres da mensagem com caracteres "chave" para formar mensagens codificadas) são os três tipos principais de transformações secretas, que podem e devem ser combinadas para aumentar o fator de trabalho necessário para decifrar um código. Este fator de trabalho depende, entre outros, dos seguintes critérios:

1. Tamanho da Chave - As chaves necessitam de espaço de armazenagem, devem ser protegidas, têm de ser comunicadas para estações remotas e introduzidas no sistema, e podem mesmo requerer memorização.
   Embora geralmente pareça desejável uma chave pequena , uma melhor proteção pode ser obtida com uma chave tão grande quanto a própria mensagem.

2. Tamanho do Espaço para a Chave - O número de transformações de segurança disponíveis deve ser tão grande quanto possível para desencorajar qualquer tentativa na base de "tente-erre-tente", bem como para permitir a atribuição de chaves únicas para um grande tipo de usuários , trocando-se as chaves a intervalos frequentes.

3. Complexidade - O custo de implantação do sistema de segurança é afetado pela necessidade de mais hardware ou tempo de processamento, mas o fator de trabalho pode também ser melhorado.

4. Sensibilidade do Êrro - O efeito de erros de transmissão ou defeitos de processamento pode tornar a decodifica -

ção impossível.

Outros critérios são, é claro, os requisitos de custo de implantação e de tempo de processamento que dependem, em parte, de estarem envolvidos o canal de comunicação ou os arquivos do sistema.

As transformações de segurança podem ser executadas através de um software adequado nos terminais e processadores centrais.

Quando desejável, ao invés disso, poderia ser usado hardware (Lucifer - IBM).

Outras contra-medidas para ameaças à segurança de informação são as sugeridas por Peterson e Turn, denominadas tratamento de ameaças.

III.4. Tratamento de Ameaças

Preocupa-se com a detecção de tentativas ou reais penetrações no sistema de arquivos, seja para fornecer uma resposta em tempo real, por exemplo solicitando o cancelamento do trabalho ou iniciando rotinas de busca, seja para permitir uma análise "post-facto". O tratamento de ameaça pode incluir a gravação de todas as tentativas rejeitadas para entrar no sistema ou em arquivos específicos, utilização de rotinas de acesso ilegais, atividade fora do comum envolvendo um determinado arquivo, tentativas de gravação em arquivos protegidos, tentativas de execução de operações restritas tais como cópia de arquivos, períodos muito longos de utilização, etc.

Relatórios periódicos para os usuários sobre atividades no arquivo podem revelar mal uso ou falsificação, e provocar uma imediata auditoria escalonada, juntamente com uma possível resposta em tempo real.

O tratamento de ameaças também ajudará a aumentar a eficácia do sistema, através de relatórios de utilização muito difundida de facilidades específicas do sistema.

Essas facilidades podem ser aperfeiçoadas ou, se fôr necessário podem ser alteradas para eliminar engarrafamentos.

Se alguma restrição de segurança estiver interferindo indevidamente na operação do sistema, o tratamento de ameaças ajudaria a assinalar essa restrição.

A tabela (3) dá um resumo, preparada por Peterson e Turn , das contra-medidas para ameaças contra a integridade da informação.

Uma boa política, em caso de tentativas de infiltração num arquivo, seria o sistema detectar e enviar ao infiltrante informações pré-determinadas, porém falsas, para dar tempo a se descobrir a origem de tal irregularidade e se tomarem as medidas cabíveis para o caso.

III.5. Restrições de Processamento

Uma sugestão para proteção de memória inclui a montagem de arquivos removíveis em unidades com circuitos desativadores que devem ser autenticados antes do acesso, apagamento de memória a

pós colocação do programa e de seus dados em um equipamento de memória auxiliar, e códigos construídos em hardware, que os equipamentos periféricos transmitiriam para outros componentes do sistema quando necessário. Um software que limita os direitos de acesso por terminal também faz parte de vários sistemas.

Tab. 3

RESUMO DE CONTRA-MEDIDAS PARA AMEAÇAS À SEGURANÇA DE INFORMAÇÃO

contra-medida / ameaça	transformações de segurança	tratamento de ameaças (audits, logs)
acidental: erro do usuário	nenhuma proteção se depender de palavra-chave; em caso contrário boa proteção.	identifica a "propensão a acidentes"; fornece conhecimento post-facto de possíveis perdas.
erro de sistema	boa proteção em caso de erros de chaveamento do sistema de comunicação.	pode auxiliar na diagnose ou fornecer conhecimento post-facto.
deliberado passivo: metodos eletromagnéticos	reduz suscetibilidade; o fator de trabalho determina a quantidade de proteção.	nenhuma proteção
gravação em fita	reduz suscetibilidade; o fator de trabalho determina a quantidade de proteção.	nenhuma proteção
deliberado ativo: "intimidação" (browsing)	boa proteção	identifica tentativas mal-sucedidas; pode fornecer conhecimento post-facto ou operar alarmas em tempo real.
"falsificação"	nenhuma proteção se depender, de palavra-chave; em caso contrário, suficiente.	identifica tentativas mal-sucedidas; pode fornecer conhecimento post-facto ou operar alarmas em tempo real.

Cont. Tab. 3

RESUMO DE CONTRA-MEDIDAS PARA AMEAÇAS À SEGURANÇA DE INFORMAÇÃO

contra-medida / ameaça	transformações de segurança	tratamento de ameaças (audits, logs)
entrada "entre-linhas"	boa proteção se as transformações de segurança forem trocadas em menos tempo do que o fator de trabalho.	análise post facto de atividade pode indicar possíveis perdas.
entrada "ilegal" (piggy back")	boa proteção se as transformações de segurança forem trocadas em menos tempo do que o fator de trabalho.	análise post facto de atividade pode indicar possíveis perdas.
entrada por pessoal do sistema	fator de trabalho, a menos que dependa de palavra-chave e falsificação é bem sucedido.	análise post facto de atividade pode indicar possíveis perdas.
entrada via "portas falsas"	fator de trabalho, a menos de acesso a obtenção de chaves.	possíveis alarmas, análise post facto.
descarga de memória com vistas a inf. residual	nenhuma proteção a menos de exequibilidade de codificação do processamento.	possíveis alarmas, análise post facto.
aquisição física de arquivos removíveis.	fator de trabalho, a menos de acesso a obtenção de chaves.	formulário de conhecimento post facto (sic) de auditoria de movimentação do pessoal.

Cont. Tab. 3

contra-medida / ameaça	controle de acesso (palavra-chave, autenticação, autorização)	restrições de processamento (armazenagem, proteção de operações privilegiadas)
acidental erro de usuário	boa proteção, a menos que o erro produza a palavra-chave correta.	reduz suscetibilidade
erro de sistema	boa proteção, a menos que ultrapassado devido ao erro	reduz suscetibilidade
deliberado, passivo: método eletromagnéticos	nenhuma proteção	nenhuma proteção
gravação em fita	nenhuma proteção	nenhuma proteção
deliberado, ativo: "intimidação" (browsing)	boa proteção (pode tornar necessário máscara)	reduz a facilidade para obtenção de uma dada informação
"falsificação"	deve conhecer as palavras-chave de autenticação (fator de trabalho para obtê-las)	reduz a facilidade para obtenção de uma dada informação
entrada "entre linhas"	nenhuma proteção, a menos que para cada mensagem, a contra-medida for usada.	limita o infiltrador ao mesmo potencial que possui o usuário de cuja linha ele compartilha
entrada "ilegal" ("piggy back")	nenhuma proteção, mas autenticação reversa (processador-para-usuário) pode ajudar	limita o infiltrador ao mesmo potencial que possui o usuário de cuja linha ele compartilha

cont. Tab. 3

contra-medida / ameaça	controle de acesso (palavra-chave, autenticação, autorização)	restrições de processamento (armazenagem, proteção de operações privilegiadas)
entrada por pessoal do sistema	pode precisar de máscara	reduz a facilidade para obtenção de uma dada informação
entrada via "portas falsas"	nenhuma proteção	provavelmente, nenhuma proteção
descarga de memória com vistas a inf. residual	nenhuma proteção	limpa áreas provadas de memória no momento de permuta
aquisição física de arquivos removíveis	não se aplica	não se aplica

IV. TÉCNICAS DE TRANSFORMAÇÕES DE SEGURANÇA

IV.1. Identificação do problema

Há um número variado de transformações de segurança, desde o método tradicional de criptografia, métodos matemáticos, até os mais recentes métodos de criptografia computacional.

Estas transformações oferecem diversas vantagens. Uma delas, se alguém tem possibilidade de entrar sub-repticiosamente em um arquivo, mas não tem a chave necessária para a decodificação, é trabalho perdido. Basicamente, transformação de segurança eleva o preço da infiltração a um custo superior ao custo próprio da informação protegida.

Usualmente o equilíbrio CPU-I/O não é afetado adversamente com a adição de transformações de segurança.

As tentações de copiar arquivos são muito mais desencorajadoras se os arquivos não são realmente decodificados.

Transformações de segurança oferecem, ainda, alguma proteção contra pessoas que podem-se tornar intrusos, em virtude de suas posições, tais como administrador do sistema, operador ou engenheiros de manutenção. Aquele último sendo obviamente o mais perigoso, conhecendo melhor a máquina que qualquer outro.

IV.2. Criptografia Clássica

Tentaremos aqui relatar quase todos os métodos de criptografia clássica.

Embora essas técnicas tenham surgido bem antes do advento do computador, sendo portanto muitas delas não adequadas para aplicação, o seu tratamento nos mostrará as possibilidades e fraquezas de cada uma, e ao mesmo tempo indicará métodos de realização em baixo nível de segurança.

A razão pela qual a criptografia tradicional não é conveniente para a computação deve-se ao fato de os arquivos dos computadores terem uma grande quantidade de repetições. Os formatos das gravações são usualmente similares e tudo isso daria ao "inimigo" a possibilidade de quebrar o método criptográfico, isto é, a mensagem codificada seria descoberta.

Definições de Termos

Vamos definir certos termos que usaremos constantemente daqui em diante.

Texto (ou mensagem) original-	mensagem a qual queremos transformar.
Criptograma-	mensagem transformada, codificada.
Criptoanálise-	estudo da resolução de um criptograma sem a posse da chave.

Inimigo- pessoa não autorizada à posse de informações ou mensagem (plaintext).

Vamos também introduzir os têrmos:

Criptagem- processo de transformar uma mensagem em criptograma.

Decriptagem - processo inverso.

Nulo- caracter sem qualquer efeito na mensagem.

Chave- a chave é que indicará as regras dentro de um método.

Classificação

A codificação, por técnicas de criptagem clássica é dividida em três grandes grupos.

1. Ocultamento ou camuflagem
2. Transposição
3. Substituição

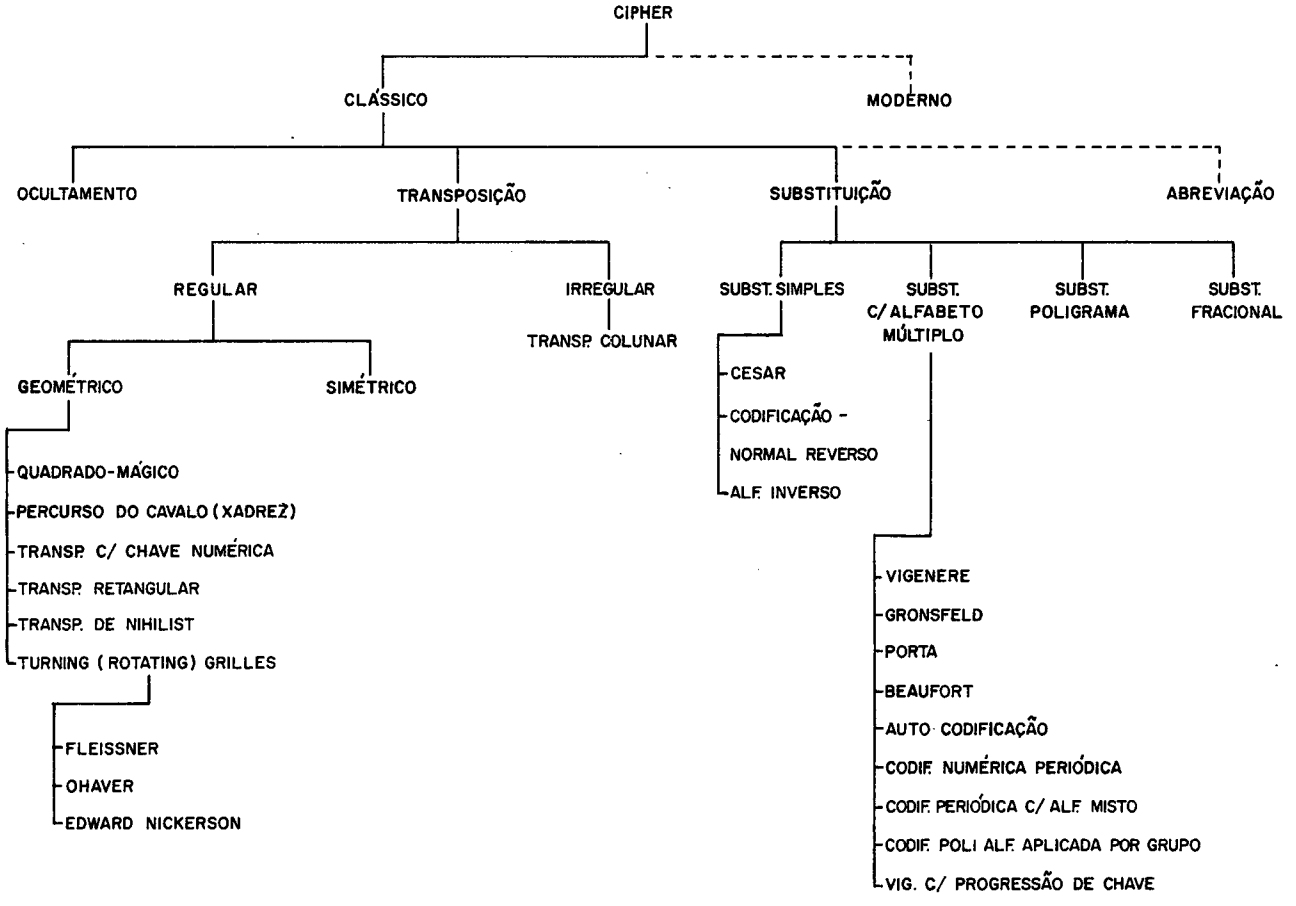
Ocultamento - os caracteres que representam a mensagem original estão escondidos ou disfarçados por um método qualquer.

Esse tipo, regra geral, serve para passar mensagens sem suspeita de tratar-se de comunica -

ção secreta.

Transposição - os caracteres da mensagem original são remanejados em sua ordem seguindo um plano pré-estabelecido.

Substituição - os caracteres da mensagem original são substituídos por outros, segundo a chave.



Árvore criptografia-clássica

IV.3. Métodos Clássicos de Criptografia

1. Camuflagem (concealment)

Talvez seja a maneira mais antiga de escrever mensagens secretas, podendo ser utilizada de várias formas.

Vejamos alguns textos com o método aplicado.

ON PEUT ÊTRE NAPOLEON SANS ÊTRE SON AMI, MES ENFANTS

Texto secreto transmitido: OPEN SESAME

Tomam-se as letras iniciais de cada palavra.

DO NOT SEND FOR ANY SUPPLIES BEFORE MONDAY, AT EARLIEST. ORDER ONCE ONLY, AS MEN IN CHARGE ARE FEELING SORE ABOUT YOUR THREAT TO ENCOURAGE THE MUTINY AT FORD'S - Wilson.

Texto secreto transmitido: SEND SUPPLIES AT ONCE.
MEN ARE ABOUT TO
MUTINY. Wilson

Este método não é conveniente para sistemas secretos "computarizados".

Uma das razões principais é o exagerado aumento de tamanho da mensagem que se quer transmitir.

2. Transposição

De acordo com o anteriormente explicado, este método consiste em desarranjar a posição relativa dos caracteres da mensagem original, segundo uma chave.

A transposição pode ser encontrada em todo grau de complexidade imaginável.

Para a preparação do criptograma há duas operações distintas:

a) escrita dos caracteres da mensagem original em blocos.

b) tomada desses caracteres segundo a chave.

Tipo Regular Geométrico

Baseia-se em tomar "unidades" pequenas ou ciclo de caracteres, e aplicar o método de transposição repetidas vezes. Toda unidade tem exatamente o mesmo número de caracteres e igual desarranjo das mesmas.

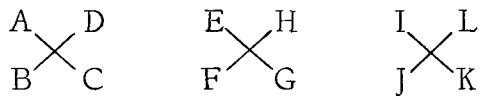
O texto é dividido em "unidades". Cada unidade será composta de uma certa quantidade de caracteres. No caso da mensagem não ser divisível por aquele número que compõe a unidade, adicionamos caracteres nulos, tantos quantos forem necessários.

O modo de se fazer a escrita dos caracteres na formação do criptograma segue de acordo com a chave.

Algumas delas formam exatamente uma figura geométrica,

tal como triângulo, quadrado, cruz, etc., se compararmos com a maneira de escrevermos o criptograma.

A fig. (3) ilustra o fato.



Texto: A B C D E F G H I J K L M N O P.

Criptograma (a) A D B C E H F G I L ...

(b) A D E H I L M P B C ...

A fig. (3)(temos uma mensagem imaginária representada por A B C D...P)mostra uma das muitas possibilidades, no caso um cruzamento simples é usado como chave, para a operação de "escrita". Logo abaixo, dois dos muitos criptogramas que podem ser "tomadas" daquele arranjo.

A unidade aqui é 4, a primeira unidade contém as letras A B C D, a segunda E F G H, e assim sucessivamente.

A mais popular das figuras geométricas é o quadrado, dividido em células, como um tabuleiro de xadrez.

O quadrado mágico é uma das denominações dadas a um desses tipos. É composto de uma série de números, 1 a 25 ou 1 a 36, etc., colocados dentro das células de tal modo arranjados que a soma tanto nas linhas, colunas, quanto nas diagonais somam um mesmo valor. Sendo esses números uma série, constitue a or-

dem, a qual, uma vez gravada, pode ser reconstituída para escrita e tomada de unidades de 25, 36, etc, caracteres.

Um outro tipo é o chamado percurso do cavalo, por lembrar o caminho permitido à peça (cavalo) do xadrez.

É baseado no tabuleiro de xadrez, com 64 células (fig.4). O percurso consiste em, se partindo de um canto, percorrer todas as células.

O primeiro caracter é colocado na célula nº 1, o segundo na nº 2 e assim por diante.

O criptograma pode ser de várias formas, tomando-se horizontalmente, verticalmente, etc, os caracteres nas linhas ou colunas do quadrado.

Fig.4

3

2

(1)	4	53	18	55	6	43	20
52	17	(2)	5	38	19	56	7
3	64	15	54	31	42	21	44
16	51	28	39	34	37	8	57
63	14	35	32	41	30	45	22
50	27	40	29	36	33	58	9
13	62	25	48	11	60	23	46
26	49	12	61	24	47	10	59

Transposição com chave numérica é mais um tipo de transposição geométrica. Em uma "unidade" de caracteres é feito o rearranjo de acordo com a chave.

A B C D E F G H I J K L ...

Chave 621435

Criptograma F·B A D C E L H G J I K ...

Uma forma muito comum de transposição geométrica está indicada na figura (5), onde uma pequena mensagem: ISTO É UMA TRANSPOSIÇÃO GEOMÉTRICA MODELO QQQQ (36 letras mais 4 nulos), está escrita dentro do bloco em uma ordem e tomada em outra.

A escrita e a tomada, ambas seguem um determinado caminho, por isso mesmo denominado transposição de rota ou transposição retangular.

Fig. 5

I	S	T	O	E
U	M	A	T	R
A	N	S	P	O
S	I	C	A	O
G	E	O	M	E
T	R	I	C	A
M	O	D	E	L
O	Q	Q	Q	Q

Criptograma:

a) Caminho descendente, início à esquerda

I U A S G T M O S M N I E R ...

b) Caminho alternado vertical, início à direita no topo.

E R O O E A L Q Q E C M A P T O T ...

c) Caminho diagonal

I U S A M T S N A O G I S ...

Três, das muitas rotas estão mostradas nos criptogramas a, b e c.

Há vários caminhos possíveis para escrever ou tomar o texto. Assim, podemos fazê-lo horizontalmente, horizontalmente reverso, horizontalmente alternado, ascendentemente, descendentemente, etc.

Para todos eles o ponto de partida é um dos quatro "corners", exceto no caso de espiral, o qual é mais adequado iniciar pelo caráter central.

Esses modelos descritos não são de alto fator de segurança, visto que processam poucas quantidades de informação, quando não feitos computacionalmente.

Transposição de Nihilist

Chave A chave é literal, mas cada letra tem um correspondente valor numérico. Assim a letra A tem valor 1, B o valor 2, etc; se não houver a letra A, ponderamos B com 1, e assim por diante.

Se a chave tiver mais que uma letra repetida, a letra mais a esquerda terá o valor menor; a outra terá o valor imediatamente superior e assim sucessivamente. Consequentemente todos os outros valores estarão modificados. Por exemplo, seja a chave AMANHÃ. Os valores numéricos correspondentes serão: 1 5 2 6 4 3.

Transposição: Consiste em aplicar a chave tanto nas linhas quanto nas colunas do bloco onde foi escrito a mensagem.

Teoricamente é uma transposição dupla.

Primeiramente escreve-se a mensagem em um bloco com tantas colunas quantos forem os caracteres da chave.

Transpõem-se então as colunas de acordo com a chave; a primeira coluna sob o valor 1, a segunda sob o valor 2 e assim seguidamente.

A segunda transposição efetua-se da seguinte maneira:
A coluna sob o número 1 intercepta a linha número 1 em cuja célula colocamos o primeiro caráter da coluna sob o número 1.

Essas intersecções serão sob o número 1 com linha 1, linha 2, linha 3, etc; coluna sob o número 2 com linha 1, linha 2, etc.

Fig. 6

Exemplo:

Palavra chave - SCOTIA
Número Associado - 524631

Bloco de Mensagem

L	E	T	U	S	H
E	A	R	F	R	O
M	Y	O	U	A	T
O	N	C	E	A	B
O	U	T	J	E	W
E	L	S	X	X	X

Primeira transposição (colunas)

	S C O T I A
	5 2 4 6 3 1
S 5	S E U H T L (primeira letra a ser transposta)
C 2	R A F O R E
O 4	A Y U T O M
T 6	A N E B C O
I 3	E U J W T O
A 1	X L X X S E (primeira posição, celula, a receber)

Segunda transposição (linhas)

E U J W T O
R A F O R E
A N E B C O
X L X X S E
A Y U T O M
S E U H T L (letra transposta)

Criptograma:

horizontalmente: EUJWT ORAFO REAN ...

3. Turning Grille

Também conhecido como transposição tipo geométrico rotacional,

originou-se da Itália, sendo seu inventor Girolamo Cardano.

Tipo "Fleissner" com chave de Ohaver

Fig. 7

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

		3			
				5	2
	8				
	6	9			7
	4				1

Chave: F R I E N D L Y G
3 8 5 2 7 1 6 9 4

1º Quadrado: Células - 38
2º " " 52
3º " " 71
4º " " 69 4

} Método de seleção das células

O quadrado pode ser de 2 x 2 células, 3 x 3, 4 x 4, etc ...

Com chave "Edward Nickerson"

Chave não numérica, portanto alfabética, sem repetição de caráter.

Ex.: FRIENDLYG

seqüência alfabética - D E F G I L NRY

DE no primeiro quadrilátero

FG no 2º

.

.

.

etc.

A chave fornece a sequência correta de se tomar os caracteres dentro das células, para formar a mensagem.

Transposição Irregular

Transposição colunar:

Escreve-se a mensagem original em blocos.

Blocos quadrados (número de linhas igual ao número de colunas) é menos conveniente do que blocos retangulares no qual apenas uma dimensão está restrita, permitindo que uma só chave governe mensagens de diferentes comprimentos.

A preparação do bloco está ilustrado na fig.8, sendo a chave semelhante à transposição de Nihilist.

Fig. 8

P	A	R	A	D	I	S	E
6	1	7	2	3	5	8	4
T	R	A	N	S	P	O	S
I	C	A	O	I	R	R	E
G	U	L	A	R	E	S	T
A	A	Q	U	I	X	X	X

Criptograma: RCUAN OAUSI RISET XPR ...
Início na coluna 1, se esgotar, seguir pela coluna 2 e assim sucessivamente.

3. Substituição

Codificação por substituição pressupõe a seleção de um conjunto de símbolos que podem representar as letras, palavras, ou caracteres de uma mensagem. Esses símbolos podem ser: ponto e traço do alfabeto Morse, a combinação do Braille e assim por diante.

Naturalmente vamos tratar aqui com caracteres do alfabeto escrito, normal, e acrescido de números.

A codificação por substituição pode ser classificada sob quatro principais tipos, cada qual tendo suas subdivisões e variações, e estes intercombinando com outros tipos.

1. Substituição simples, também chamada substituição monoalfabética, faz uso de somente um alfabeto de codificação.

2. Substituição com alfabeto múltiplo, também chamada de substituição com chave dupla, substituição polialfabética, etc, faz uso de diversos e diferentes alfabetos de codificação de acordo com algum plano pré-estabelecido.

   O termo multisubstitucional é algumas vezes aplicado, mas mais corretamente refere-se a certa forma de substituição simples, no qual o alfabeto simples está assim designado para providenciar substituição opcional para todos ou parte dos caracteres.

3. Poligrama - esquema no qual os grupos de caracteres são integralmente substituídos por outros grupos (letras ou números).

   Há necessidade de um dicionário de substituição, o que torna a segurança pouco eficaz.

4. Substituição fracional - requer um certo tipo de alfabeto de codificação, encontra-se um substituto para os caracteres simples e submetem-se essas frações para posterior codificação.

   Mais do que nunca, o resultado é uma combinação de codificação, mais do que puramente combinação substitucional.

Substituição Simples

É ordinariamente definido como uma codificação na qual cada caracter do alfabeto tem um substituto fixo, e cada criptograma de símbolos representa uma mensagem original fixa.

Um dos mais simples métodos de substituição é chamado de César; suposições indicam Julio César como seu criador.

Basicamente consiste em "Shiftar" o alfabeto original, tanto quanto fôr a chave.

Alfabeto original - A B C D E F G H ... X Y Z

Alfabeto codificado - D E F G H I J ..... A B C

K = 3 (chave)

Uma variação desse método:

Alfabeto de Codificação Normal Reverso.

Alfabeto original - A B C D .:. M N O P ... Y Z

Alfabeto codificado - N M L K ... B A Z Y ... P O

Outra variação:

Alfabeto inverso A B C D ... Y Z

Z Y X ..... B A

Divisão do alfabeto normal em duas metades e 'Shiftar' uma das metades:

A B C D E F G | H I J K L M

T S R Q P O N | Z Y X W V U

Alfabeto com inclusão de

Palavra-chave:

A B C D E ..... O .....Z

S T E N O G R A P H I C B D F J K L ...Z

Substituição com Alfabeto Múltiplo :

Tipo Gronsfeld.

O alfabeto é governado por chave numérica.

Codificação Gronsfeld

Chave	2	8	1	0	5	2	8	1	0	5	2	8	...
Mensagem Original	S	E	N	D	S	U	P	P	L	I	E	S	...
Criptograma	U	M	O	D	X	W	X	Q	L	N	G	A	

É identico a codificação Vigenère com a chave CIBAF; U é o substituto de S no alfabeto (C) CDE ..... ZAB; M o substituto de E no alfabeto (I) IJK .....H, etc.

Desta forma temos somente 10 alfabetos de substituição.

Note-se que S sendo o 19º caráter , U é (19 + 2)º carácter, e assim por diante.

Método de Vigenère

Um conjunto de 26 alfabetos compõe a tábua de Vigenère.

Cada caráter a ser criptado utiliza um determinado alfabeto, que depende da chave usada.

A figura 9 apresenta a tabela (ou tábua) de Vigenère, também chamada quadro de alfabeto.

O caráter da mensagem original é encontrado no alfabeto horizontal (A B C ... Z) e o alfabeto utilizado para a criptagem é encontrado de acordo com o correspondente caráter da chave na vertical.

Fig. 9

TÁBUA DE VIGENÈRE

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Exemplo:

Chave : C H A C H A C H A C H A C ....

M. or. : I S S O E A M E N S A G E ....

Cript. : K Z S Q L A O ....

Para se obter a mensagem original a partir do criptograma, procede-se da seguinte forma:

a) pela chave obtem-se o alfabeto

b) procura-se nesse alfabeto o caráter correspondente ao caráter do criptograma

c) encontrando-o sobe-se verticalmente na tábua e encontra-se o caráter da mens. orig.

Do exemplo anterior:

Chave: C H A C H A ....

Cript.: K Z S ....

M. or.: I S S ....

Note-se que no exemplo, com a chave C H A utilizamos apenas 3 alfabetos dos 26 disponíveis.

Existe um modelo matemático muito simples que representa este método de codificação.

Se as letras do alfabeto forem designadas com valores numéricos (A = 0, B = 1, ... Z = 25), a combinação de uma coluna com uma linha for definida como "adição", e o caracter da intersecção definida como "soma", então a codificação consiste em uma adição módulo 26.

De acordo com isso: 21 + 7 = 2 ou

V + H = C

Sob essa soma modular, o alfabeto constitue um caso espe-

cial de grupo Abeliano comutativo.

- Porta

São treze alfabetos de substituição, cada um governado por dois caracteres.

Em todos os treze alfabetos a codificação é recíproca (isto é, um caráter corresponde ao outro, assim como este corresponde ao primeiro).

Por exemplo, no alfabeto A B o substituto de A é N e o de N é A.

O caráter da chave determina o alfabeto.

Codificação Porta:

Chave: E A S T E A S T ....

Mens.: S E N D S U P P ....

Crip.: D R E Z D H G G

Pode haver um mesmo criptograma para uma outra chave. Seja a chave F A T S

Chave: F A T S F A T S ....

Mens.: S E N D S U P P ....

Cript.: D R E Z D H G G ....

TABELA DE PORTA

AB	A	B	C	D	E	F	G	H	I	J	K	L	M
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CD	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	P	Q	R	S	T	U	V	W	X	Y	Z	N
EF	A	B	C	D	E	F	G	H	I	J	K	L	M
	P	Q	R	S	T	U	V	W	X	W	Z	N	O
GH	A	B	C	D	E	F	G	H	I	J	K	L	M
	Q	R	S	T	U	V	W	X	Y	Z	N	O	P
IJ	A	B	C	D	E	F	G	H	I	J	K	L	M
	R	S	T	U	V	W	X	Y	Z	N	O	P	Q
KL	A	B	C	D	E	F	G	H	I	J	K	L	M
	S	T	U	V	W	X	Y	Z	N	O	P	Q	R
MN	A	B	C	D	E	F	G	H	I	J	K	L	M
	T	U	V	W	X	Y	Z	N	O	P	Q	R	S
OP	A	B	C	D	E	F	G	H	I	J	K	L	M
	U	V	W	X	Y	Z	N	O	P	Q	R	S	T
QR	A	B	C	D	E	F	G	H	I	J	K	L	M
	V	W	X	Y	Z	N	O	P	Q	R	S	T	U
ST	A	B	C	D	E	F	G	H	I	J	K	L	M
	W	X	Y	Z	N	O	P	Q	R	S	T	U	V
UV	A	B	C	D	E	F	G	H	I	J	K	L	M
	X	Y	Z	N	O	P	Q	R	S	T	U	V	W
WZ	A	B	C	D	E	F	G	H	I	J	K	L	M
	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
YZ	A	B	C	D	E	F	G	H	I	J	K	L	M
	Z	N	O	P	Q	R	S	T	U	V	W	X	Y

Beaufort.

Semelhante à tabela de Vigenère, temos a tabela de Beaufort.

TABELA DE BEAUFORT

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

É uma tabela 27 x 27 elementos, todo o alfabeto A B .... Z está nas quatro arestas. Usam-se palavras chaves também, como nos anteriores, para codificar a mensagem.

Chave: C O M E T ....

Mens.: S E N D S ....

Crip.: K K Z B B ....

Para substituir S, com o uso do caráter chave C, toma-se S em um dos quatro alfabetos dos cantos. Segue-se em linha na coluna de S (ou linha de S) até a letra C, neste ponto dobra-se em ângulo reto até encontrar o caráter substituto no alfabeto dos cantos.

Dessa maneira estamos dentro das características da codificação Beaufort.

Uma variante desse método é se tomar primeiro o caráter da chave, ao invés do caráter da mensagem. Para se encontrar o substituto do caráter faz-se da mesma forma anterior.

Assim, a mensagem acima ficaria assim:

Chave: C O M E T ....

Mens.: S E N D S ....

Crip.: Q Q B Z Z ....

- Auto-codificação

Este método usa uma das técnicas de codificação com alfa -

beto múltiplo (usualmente Vigenère); tal como ilustra o exemplo.

Vigenère Autokey: C O M E T S E N D S U P P L I E S ....

Original: S E N D S U P P L I E S T O ....

Criptograma: U S Z H L M T C ....

C O M E T é a chave inicial. A chave será do tamanho da mensagem menos a chave inicial.

Para se tornar mais dificil a decriptagem podemos aplicar o método novamente. Agora a chave será o criptograma anterior, precedido pela chave própria, no caso C O M E T.

Chave: C O M E T U S Z H L ....

Mens.: S E N D S U P P L I E S ....

Cript.: U S Z H L O H O S T ....

- Codificação com números periódicos

Um exemplo:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

I ≡ J

Chave COMETA

13 34 32 15 44 11

Mens.:	S E N D S S U P P L I E S ....
Texto modif.:	43 15 33 14 43 45 35 35 31 24 15 43 ....
Chave periódica:	13 34 32 15 44 11 13 34 ....
	56 49 65 29 87 58 69 67 ....

Este método não é conveniente pois aumenta em dobro o número de caracteres. (A cada letra correspondem dois dígitos).

- Vigenère com Chave em Progressão

Exemplos de chaves em progressão:

A B C D E F .... Z	índice de progressão 1
A C E G I K .... Z | B ... Y	índice de progressão 2
A Z Y X W V U T S R	índice de progressão 25 (mod. 26)

CULPEPER	DVMQFQFS	EWNR....	
C	D	E	índice de progressão = 1

O método é o mesmo do esquema Vigenère ou Beaufort visto anteriormente, apenas a chave segue um esquema pré-determinado.

Note-se que quando a chave progride no alfabeto, o possível substituto para cada carácter também progride exatamente da mesma maneira.

Progressão Vigenère, Beaufort e Variante Beaufort:

Chave em progressão (índice 1)	A B C D E F
Mens. original	H H H H H H
Criptograma (Vig.)	H I J K L M
(Beauf.)	T U V W X Y....
(Var.)	H G F E D B

No método Vigenère e Beaufort a progressão é no mesmo sentido do alfabeto, enquanto que na Variante Beaufort, a progressão é no sentido inverso.

Tal fato pode ajudar a decriptagem, então um método a dar maior segurança é criptar primeiramente a mensagem original do modo convencional (Vigenère) e depois criptar o criptograma com uma chave em progressão tomando-se grupo por grupo.

Chave inicial	CULPEPER	CULPEPER	CUL ....
M. original	THEREISO	THERCAUS	EFO ....
Cript.inicial	VBPGIXWF	VBPGGPYJ	GZZ
Chave em progressão	A	B	C
Cript. final	VBPGIXWF	WCQHHQZK	IBB ....

- Substituição Poligrama:

Substituição de diversos caracteres coletivamente, diagrama por diagrama, triagrama por triagrama, etc.

Muitas tabelas podem ser construídas para essa substituição.

A do tipo mais comum é a tabela mostrada abaixo:

	A	M	E	R	I	C	N	B	D	F	G	H	J	K	L	O	P	Q	S	T	U	V	W	X	Y	Z
Ê	AA	BA	CA	DA	EA	FA	GA	HA	IA	JA	KA	LA	MA	NA	OA	PA	QA	RA	SA	TA	UA	VA	WA	XA	YA	ZA
Q	AB	BB	CB	DB	EB	FB	GB	HB	IB	JB	KB	LB	MB	NB	OB	PB	QB	RB	SB	TB	UB	VB	WB	XB	YB	ZB
U	AC	BC	CC	DC	EC	FC	GC	HC	IC	JC	KC	LC	MC	NC	OC	PC	QC	RC	SC	TC	UC	VC	WC	XC	YC	ZC
A	AD	BD	CD	DD	ED	FD	GD	HD	ID	JD	KD	LD	MD	ND	OD	PD	QD	RD	SD	TD	UD	VD	WD	XD	YD	ZD
L	AE	BE	CE	DE	EE	FE	GE	HE	IE	JE	KE	LE	ME	NE	OE	PE	QE	RE	SE	TE	UE	VE	WE	XE	YE	ZE
I	AF	BF	CF	DF	EF	FF	GF	HF	IF	JF	KF	LF	MF	NF	OF	PF	QF	RF	SF	TF	UF	VF	WF	XF	YF	ZF
T	AG	BG	CG	DG	EG	FG	GG	HG	IG	JG	KG	LG	MG	NG	OG	PG	QG	RG	SG	TG	UG	VG	WG	XG	YG	ZG
Y	AH	BH	CH	DH	EH	FH	GH	HH	IH	JH	KH	LH	MH	NH	OH	PH	QH	RH	SH	TH	UH	VH	WH	XH	YH	ZH
B	AI	BI	CI	DI	EI	FI	GI	HI	II	JI	KI	LI	MI	NI	OI	PI	QI	RI	SI	TI	UI	VI	WI	XI	YI	ZI
C	AJ	BJ	CJ	DJ	EJ	FJ	GJ	HJ	IJ	JJ	KJ	LJ	MJ	NJ	OJ	PJ	QJ	RJ	SJ	TJ	UJ	VJ	WJ	XJ	YJ	ZJ
D	AK	BK	CK	DK	EK	FK	GK	HK	IK	JK	KK	LK	MK	NK	OK	PK	QK	RK	SK	TK	UK	VK	WK	XK	YK	ZK
F	AL	BL	CL	DL	EL	FL	GL	HL	IL	JL	KL	LL	ML	NL	OL	PL	QL	RL	SL	TL	UL	VL	WL	XL	YL	ZL
G	AM	BM	CM	DM	EM	FM	GM	HM	IM	JM	KM	LM	MM	NM	OM	PM	QM	RM	SM	TM	UM	VM	WM	XM	YM	ZM
H	AN	BN	CN	DN	EN	FN	GN	HN	IN	JN	KN	LN	MN	NN	ON	PN	QN	RN	SN	TN	UN	VN	WN	XN	YN	ZN
J	AO	BO	CO	DO	EO	FO	GO	HO	IO	JO	KO	LO	MO	NO	OO	PO	QO	RO	SO	TO	UO	VO	WO	XO	YO	ZO
K	AP	BP	CP	DP	EP	FP	GP	HP	IP	JP	KP	LP	MP	NP	OP	PP	QP	RP	SP	TP	UP	VP	WP	XP	YP	ZP
M	AQ	BQ	CQ	DQ	EQ	FQ	GQ	HQ	IQ	JQ	KQ	LQ	MQ	NQ	OQ	PQ	QQ	RQ	SQ	TQ	UQ	VQ	WQ	XQ	YQ	ZQ
N	AR	BR	CR	DR	ER	FR	GR	HR	IR	JR	KR	LR	MR	NR	OR	PR	QR	RR	SR	TR	UR	VR	WR	XR	YR	ZR
O	AS	BS	CS	DS	ES	FS	GS	HS	IS	JS	KS	LS	MS	NS	OS	PS	QS	RS	SS	TS	US	VS	WS	XS	YS	ZS
P	AT	BT	CT	DT	ET	FT	GT	HT	IT	JT	KT	LT	MT	NT	OT	PT	QT	RT	ST	TT	UT	VT	WT	XT	YT	ZT
R	AU	BU	CU	DU	EU	FU	GU	HU	IU	JU	KU	LU	MU	NU	OU	PU	QU	RU	SU	TU	UU	VU	WU	XU	YU	ZU
S	AV	BV	CV	DV	EV	FV	GV	HV	IV	JV	KV	LV	MV	NV	OV	PV	QV	RV	SV	TV	UV	VV	WV	XV	YV	ZV
V	AW	BW	CW	DW	EW	FW	GW	HW	IW	JW	KW	LW	MW	NW	OW	PW	QW	RW	SW	TW	UW	VW	WW	XW	YW	ZW
W	AX	BX	CX	DX	EX	FX	GX	HX	IX	JX	KX	LX	MX	NX	OX	PX	QX	RX	SX	TX	UX	VX	WX	XX	YX	ZX
X	AY	BY	CY	DY	EY	FY	GY	HY	IY	JY	KY	LY	MY	NY	OY	PY	QY	RY	SY	TY	UY	VY	WY	XY	YY	ZY
Z	AZ	BZ	CZ	DZ	EZ	FZ	GZ	HZ	IZ	JZ	KZ	LZ	MZ	NZ	OZ	PZ	QZ	RZ	SZ	TZ	UZ	VZ	WZ	XZ	YZ	ZZ

A tabela apresenta 676 combinações possíveis de dois caracteres (diagrama).

Desse modo TH pode ser substituído por LG ou TN dependendo da forma que se toma na tabela.

Uma outra maneira de se montar a tabela é aquela mostrada em seguida:

Alfabeto em quadrado de 5 x 5
(J ≡ I)

L	Z	Q	C	P
A	G	N	O	U
R	D	M	I	F
K	Y	H	V	S
X	B	T	E	W

Com essa tabela o diagrama:

AC é substituído por LO (L está acima de A)
RI é substituído por DF (D ao lado de R).
F ao lado de I
RF é substituído por DR
PS é substituído por UW (U vem abaixo de P / W vem abaixo de W)

- Substituição Fracional

A substituição fracional requer um alfabeto de codificação do tipo múltiplo, isto é, um símbolo é composto de duas ou mais unidades tal como

em BACON e TRITHEMIUS (alfabetos).

Alfabeto de BACON

A	aaaa
B	aaab
C	aaaba
D	aaabb
	⋮
	etc

Alfabeto de TRITHEMIUS

A	111
B	112
C	113
D	121
	⋮
	etc

Entre outros tipos temos o chamado sistema de "Pollux", onde a base é o alfabeto do código Morse.

E.	S...	H....	B - ...
T -	U ..-	V ...-	⋮
I ..	R .-.		etc
A .-			

Método de Collon: onde a base é um tabuleiro. O texto é submetido a uma substituição convencionada por um alfabeto, e o resultado, o criptograma, é então submetido a uma transposição.

Existem vários outros métodos dentro da substituição fracionada, mas como todos eles fazem uso de um alfabeto onde cada símbolo é apresentado por dois ou mais caracteres, isto faz crescer a mensagem original.

Alguns métodos fazem uso de alfabeto múltiplo mas o criptograma final mantém as características do alfabeto do texto original.

Chave - Tabuleiro

	1	2	3	4	5
1	G	B	M	V	E
2	C	O	W	N	D
3	P	X	F	Q	Y
4	R	H	S	Z	A
5	I	T	L	K	U

Preparação do alfabeto

G	E	N	*	R	A	L
B	C	D	F	H	I	K
M	O	P	Q	S	T	U
V	W	X	Y	Z		

Substitutos: S = 43
E = 15
N = 24
D = 25

Substituição Inicial:

I	S	T	O	E	U	M	E	X	E	M	P	L	O
5	4	5	2	1	5	1	1	3	1	1	3	5	2
1	3	2	2	5	5	3	5	2	5	3	1	3	2

Re-substituição:

54 52 ..... 13 22

Criptograma: K T ..... M O

IV.4. Técnicas Criptográficas Computacionais

4.1 - Técnicas criptográficas para processamento e armazenagem em arquivos computacionais de informações confidenciais.

Vistas as técnicas tradicionais de criptografia vejamos as características necessárias para implementação de técnicas criptográficas em sistemas computacionais.

O objetivo é assegurar ao usuário de arquivos confidenciais proteção contra possíveis tentativas de infiltração de pessoa não autorizada.

Breve histórico:

Recentemente Ware (1967), Peterson e Turn (1967) fizeram estudos, com grandes detalhes, da necessidade de proteção de arquivos confidenciais, e também da maneira que essa proteção poderia ser realizada.

Tassel (1969) sugeriu diversas técnicas clássicas de criptografia como solução para esse propósito.

Todos os esquemas clássicos de criptografia foram desenvolvidos para comunicação de pequenas quantidades de dados ou mensagens em linguagem natural, durante curto período de tempo e em época pré-computador. Desta forma é justo chamá-los "comunicação criptográfica".

Por outro lado os problemas encontrados em sistemas computacionais são mais complexos naturalmente.

Grandes somas de dados e programas, quer em linguagem natural ou artificial, são para serem processados ou armazenados em arquivos, durante período de tempo maior.

Tais arquivos são passíveis de acesso não autorizado e podem ser submetidos à análise por um técnico competente e interessado.

O recurso possível para o analista são os computadores, que são velozes, tendo grande capacidade de processamento de informações, por isso mesmo sendo possível levar a cabo exaustiva análise de dados em tempo muito curto.

Desde que os fatores envolvidos aqui são radicalmente diferentes daqueles envolvidos em "comunicação criptográfica", parece desejável chamarmos a nova ciência, o qual trate com segredos e processamento de informações melindrosas em sistemas computacionais, de "criptografia computacional".

4.2 - Critério para uma perfeita codificação ou cripto-programa.

Shannon (1949)
considera o critério e medidas para o segredo e perfeição dos criptogramas de comunicação em seu trabalho.

Muitos e interessantes resultados são avaliados, a despeito do fato de ter sido escrito bem antes do advento dos computadores.

Então, muitos desses pontos de vistas, estão intimamente ligados com os métodos criptográficos manuais ou mecanicamente simples.

São especificados cinco critérios para uma perfeita codificação em criptografia de comunicação(ou comunicação criptográfica).

1 - A quantidade de "segredo" necessária decidirá a soma de trabalho para codificar e decodificar (criptar-decriptar).

2 - O conjunto de regras (ou chave) usado para tal está livre de complexidade.

3 - A implementação do processo é o mais simples possível.

4 - Erros no processo não pode se expandir causando perda de informação.

5 - O tamanho da mensagem código não se expandirá comparado com o tamanho da mensagem original.

Antes de considerarmos o critério para a perfeita codificação em criptografia computacional, é interessante discutir alguns problemas práticos encontrados na idealização de técnicas convenientes para a criptografia computacional.

Nos computadores os códigos de máquina usados são fixos e os dados precisam necessariamente es-

tar na forma adequada para a máquina.

Os caracteres de codificação (símbolos)usados precisam ser escolhidos de tal maneira que o computador seja capaz de reconhecê-los e "manuseá-los".

Desta forma qualquer código simbólico não poderá ser introduzido ao bel-prazer.

Muitos dos dados ou programas são guardados de modo convencional, em forma linear, em memórias sequenciais como fitas, discos, etc.

Então o uso de esquemas de transposição, com um alto grau de segurança, envolveria enormes somas de complexidades, tempo, trabalho e capacidade de memória. (Por ex.: transp.colunar, a bloco teria que ser muito grande, para que a transposição fosse entre caracteres bem distantes uns dos outros).

Desde que os dados ou programas (criptados) terão de ser decifrados (decriptados) de ante-mão pela máquina e também só poderão ser codificados (criptados) apenas depois que a computação estiver completa,mesmo uma simples substituição envolverá grande complexidade.

Além disso a maioria dos modernos sistemas projetados são levados a cabo usando alguma linguagem de programação disponível comercialmente.

Desta forma, se um esquema de substituição é usado, o segredo pode não ser garantido, devido a estrutura definida da linguagem usada. Também excessiva mutilação das palavras, frases e sentenças (como em camuflagem) em uma linguagem "standard", seria equivalente a usar uma nova linguagem de programação, cripto-programação; isto significaria que o trabalho de codificar e decodificar seria tão complexo quanto construir outro compilador para a linguagem de cripto-programação.

Todas as linguagens de programação tem em vista o seu fácil aprendizado, fácil para se fazer programas e comunicação também fácil entre programadores (Higman 1967). Desta forma não há meio de escapar do uso das linguagens "standard", caso contrário o custo de programação seria proibitivo.

Consequentemente alguma codificação em criptografia computacional terá de satisfazer os seguintes critérios:

1 - A quantidade ou grau de segurança decidirá o tempo de computação e trabalho de programação.

2 - A Chave usada deverá ser simples em construir, fácil de suprir à máquina, facilmente modificável e ocupará o mínimo de memória.

3 - Criptagem e decriptagem com a chave conhecida deverá ser o mais simples possível envolvendo pouco tempo de processamento.

4 - A chave destroi o parametro estatístico ou estrutura natural da linguagem.

5 - Erros na criptagem-decriptagem não deverá causar ambiguidades ou distorções no programa ou dado original, fazendo-o inutilizável.

6 - A quantidade de memória requerida para o criptograma não deverá aumentar em muito, comparado com o original.

7 - Análise do criptograma sem a chave causará um enorme problema combinacional envolvendo grande complexidade de computação.

4.3 - Técnicas avançadas de criptografia para computação.

Os arquivos computacionais oferecem algumas características peculiares para quem pretende usar a criptografia computacional.

Tais arquivos dão ao "criptanalista inimigo" uma grande quantidade de dados nos quais podem ser trabalhados.

Desde que se saiba qual o tipo de informação contida no arquivo (programa, arquivo de endereços, informações científicas), e geralmente este é o caso, se assim não fosse não haveria interesse em apoderar-se dele, torna-se mais identificável o método de ação.

Em arquivos computacionais todos os registros são usualmente similares, isto é, um arquivo de en

dereços conterá todos eles, endereços, provavelmente em sequência.

Programas em linguagem de alto nível (Fortran, Cobol) tem alta percentagem de caracteres repetidos. Pode se dizer também que a maioria das vezes, a estrutura de um arquivo pode ser adivinhado. Por exemplo, um endereço usualmente inicia cada registro com um nome, seguido do endereço, e termina com um ponteiro .

Tudo isso ajudará em muito o criptanalista a decodificar, mesmo quando técnicas sofisticadasde criptografia são usadas.

A fim de manter a segurança dos arquivos computacionais confidenciais deve-se tomar as seguintes precauções:

1) Repetições de chaves criptográficas devem ser evitados.

2) Uso de transposição e substituição e nulos ajudará a resolver o problema de repetições características de estrutura.

3) O sistema deve usar uma única chave para cada registro.
   Em arquivos sequenciais a chave pode ser calculada tomando-se por base o número de registro.
   Em arquivos não sequenciais a chave terá de ser inserida em cada registro.

4.4 - Propriedades das transformações de segurança.

Um aspécto muito importante é a unicidade da decriptagem de uma mensagem criptada. Em termos computacionais significa que dado um algorítmo de criptagem, existirá um algorítmo bem definido para decriptagem resultando na obtenção da informação original.

Em termos matemáticos é conveniente definir criptagem como uma transformação de uma mensagem original por meio de um operador. Então a condição de unicidade é que a transformação seja não-singular ou que seja de solução única.

Seja M a mensagem, K o operador e C o criptograma e escrevemos:

$C = M * K$ onde $*$ denota uma operação adequada.

Definimos K^{-1} operador inverso na expressão:

$$M = C * K^{-1}$$

4.5 - Métodos modernos de transformação de segurança.

Vamos considerar alguns operadores (K) de transformação de segurança adequadas à implementação computacional, bem como operações adequadas.

Esquemas aritméticos

a) Adição/Subtração

A operação de adição (ou subt.) apresenta operação inversa bem definida, podendo portanto servir para os nossos intuitos.

Para esse propósito, o dado ou programa, os quais estão em um sistema de $\underline{n}$ caracteres-alfabeto, são vistos como um número de um bloco de números na base $\underline{n}$, fazendo uma correspondencia, de um para um, do alfabeto a_i com o digito d_j (i=1 até n, j = o até (n-1) do código base $\underline{n}$. (É na verdade um esquema de substituição numérica).

Desde que os computadores digitais operam com números, usando um código binário para representar os caracteres alfa-numéricos, este procedimento (adição/subt.) é fácil de implementar.

Para cada substituição numérica obtém-se um adequado número K(chave) na base $\underline{n}$ que adicionado (ou subtraido) a mensagem original M resultará o criptograma C.

$$M \pm K = C$$

M é facilmente reencontrado

$$M = C \mp K$$

operação: $\pm$

b) Multiplicação/Divisão

Similarmente multiplicação ou/e divisão podem ser usadas como operações de transformação.

No caso da multiplicação, entretanto, o criptograma expandirá em tamanho, o que é uma desvantagem.

A divisão por outro lado apresenta a vantagem de diminuir o tamanho, quando a chave é grande, no entanto devemos ter K como um divisor perfeito.

Esta técnica serve-se muito bem quando há uma grande quantidade de dados a ser armazenado e para ser recuperado usando uma chave simples.

É também conveniente usar como operador p/q (onde p e q são inteiros bem definidos).

Tendo em vista o fato de que algorítmos numéricos rapidíssimos estão disponíveis para operações aritméticas de comprimento-múltiplo, este procedimento é altamente adequado para a computação.

c) Mudança de base

Conversão e reconversão são únicos para números inteiros, logo é uma outra técnica disponível.

Algorítmos rápidos e simples existem para mudança de base.

A grande vantagem dos esquemas aritméticos é a simplicidade na implementação.

A probabilidade de adivinhar os operan-

dos a partir do resultado de uma operação aritmética é extremamente baixa; então um típico parâmetro estatístico envolvido em uma linguagem, tal como a frequência de letras, diagramas, triagramas, % de vogais, etc., é destruído por esta técnica.

A principal desvantagem, entretanto, é o fato de que se algum erro ocorrer durante a criptagem, mesmo um simples dígito, é o bastante para destruir completamente a mensagem.

Entretanto, a probabilidade de tal erro é muito baixa. Há também bons métodos para correção em operações aritméticas, fazendo portanto o esquema aritmético altamente adequado.

Esquemas Lógicos.

Operações lógicas ou Booleanas são possíveis para uso em criptografia computacional.

Dentre as 16 operações binárias da álgebra Booleanas somente a Negação (-), Equivalencia ($\equiv$) e o Or-Exclusivo ($\oplus$, soma módulo 2) possuem operação inversa. Todas as outras, And ($\wedge$), Or ($\vee$), Nand(/),Nor ($\uparrow$), Implicação ($\rightarrow$), etc., não tem inverso.

Seja M sequência de O's e 1's (código binário),

K a chave de mesmo comprimento.

Então: $M \wedge K = C$ e não há meio de re-

cuperar M de C, dado K. A operação And, destroi M completamente. Entretanto com o uso de operações de Or-Exclusivo, Eq. ou Neg. podemos recuperar M.

Então se $C = (M \oplus K)$, $M = (C \oplus K)$

ou se $C = \overline{M}$, $M = \overline{C}$

e se $C = (M \equiv K)$

$M = (C \equiv K)$

Este princípio pode ser usado muito eficazmente na decomposição de um arquivo M em dois (ou mais) arquivos C_1 e C_2, tal que M não pode ser reencontrado, a menos que os arquivos componentes C_1 e C_2 sejam adequadamente compostos na presença da chave K:

Ex.:

(1) $M \vee K = C_1$

$\overline{M} \vee \overline{K} = C_2$

então

$M = (C_1 \wedge C_2) \oplus K$

(2) $M \rightarrow K = C_1$

$K \rightarrow M = C_2$

então

$M = (C_1 \wedge C_2) \equiv K$

(3) $M \wedge K = C_1$

$\overline{M} \wedge \overline{K} = C_2$

$$M = (C_1 \vee C_2) \equiv K$$

④ $M \wedge K = C_1$

$M \vee K = C_2$

$M = (C_2 \rightarrow C_1) \equiv K$

Muitas outras combinações podem ser construidas. Este esquema é seguro desde que haja duas chaves envolvidas na operação binária e a chave K.

Esquema Matricial

Mais interessante mas mais trabalhoso é o esquema de uso de matrizes.

O caráter do alfabeto é transformado em código binário de p dígitos e então arranjado adequadamente como elemento (cada dígito) de uma matriz retangular com r linhas e s colunas.

Introduz-se elementos redundantes no caso de $p < rs$.

Esta matriz M pode então ser multiplicada ou somada com uma outra matriz K adequadamente escolhida como chave.

A técnica de adição, embora envolvendo menor quantidade de operações matemáticas tem a desvantagem de ser tão grande quanto M, a chave K.

No caso da multiplicação, K tem um único inverso; desta forma precisamos escolher uma matriz quadrada não-singular para K.

Para também reduzir o trabalho computacional, é preferível que M tenha um número de linhas r maior do que o número de colunas, em suma muitas linhas e poucas colunas.

Isto porque multiplicamos a matriz M (r x s) por K (s x s). O número de multiplicações necessárias é rs^2 e o número de adições é rs(s-1). Consequentemente é aconselhável fatorizar p=rs de tal modo que r seja grande e s pequeno.

Então tem-se, a mais, a vantagem de K ser pequeno e cujo inverso pode ser imediatamente computado ou armazenado.

Em alguns casos simples a matriz K pode ser escolhida de tal modo que K^{-1} é sua transposta, são as matrizes ortogonais. Matrizes de Hadamard são grandemente úteis. Tais matrizes têm elementos que são +1 ou -1 e seu inverso é a transposta dividido pela ordem da matriz (2). Se portanto a ordem de K for escolhida adequadamente como potência de 2 a criptagem e decripitagem tornará extremamente simples.

Outra classe de matrizes adequado para o trabalho criptográfico são as matrizes cujos elemen -

tos são 1 e 0, e o seu inverso apresenta 1, 0 ou - 1 (1).

Exemplos de matrizes K.

1) $K = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \qquad K^{-1} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & -1 \\ 0 & 1 & -1 & -1 \end{bmatrix}$

2) $K = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \qquad K^{-1} = \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$

- Esquemas Topológicos, Funcionais.

Existem outros esquemas que aparece - ram enraizados a semelhança de esquemas clássicos de transposição.

Os dados ou programas, a serem crip - tados, são segmentados em partes e arranjados como conteudos de uma célula claramente numerada (endereçada), ou de uma matriz, de alguma forma geométrica. (Veja transposição clássica).

A criptagem pode ser então construída de dois diferentes métodos.

O primeiro método, escolhe se um caminho satisfazendo uma certa relação funcional simples nos

endereços e o conteúdo são re-arranjados ou transpostos na sua ordem.

Este método poderia ser ao esquema "Standard" de processamento de endereços.

A relação funcional simples serve como chave.

No segundo método adota-se um caminho topológico mais complicado que o anterior, não necessariamente satisfazendo a relação de endereços.

Um mapa e um apontador (pointer) são as chaves.

O mapa pode ser guardado como uma descrição envolvendo "heads", "links" e "fim de listas". É um método semelhante a técnica de processamento de listas (list-processing-Knuth)

V. DECRIPTAGEM

Para os métodos clássicos de criptografia existe para cada método específico uma correspondente técnica de decriptagem sem o conhecimento da chave, que melhor se adapta à solução.

Assim para o método de transposição regular temos a chamada solução de Givierge, para técnicas de substituição podemos ter soluções por frequência, terminal de sequências, contagem de contactos, frequência de vogais, etc.

A tabela 4 mostra para cada tipo de criptagem o correspondente método de solução.

Talvez a arma mais poderosa para solucionar criptogramas seja o parametro estatístico.

Conhecendo-se a frequência de uso dos caracteres, como é conhecido por exemplo a frequência das letras na linguagem inglesa, espanhola, portuguesa, francesa, etc, bem como os diagramas, triagramas, frequência de vogais, pode-se fazer uma estatística do criptograma e comparar com aquelas tabelas pré-determinadas e assim descobrir a chave e toda a mensagem codificada.

No anexo (3) apresentamos algumas linguagens e suas frequências (letras, diagramas e vogais).

É claro que a maior ou menor facilidade de decriptagem não está só no método usado de criptagem, mas também na qualidade da chave do método.

Repetido uso de uma chave em combinação linear é o tendão de Aquiles de tal sistema, e chaves predizíveis também é outra fraqueza do sistema.

Se a chave é randômica, tão longo quanto a mensagem a criptar, e destruido após o seu uso, o resultado do criptograma poderia ser inquebrável, em teoria.

A verdade, é que codificações "inquebráveis" praticamente não existem.

Para textos curtos o uso de chave uma vez só é realizável, mas para textos muito grandes o uso de chaves "one-time key" não é prático, nem econômico.

Em textos moderados tal tática pode ser empregada; mas como o tráfico da mensagem aumenta, a sua circulação torna-se uma necessidade prática.

Isto é, a chave é muitas vêzes usada e a codificação se torna vulnerável.

Bryant Tuckerman (IBM) mostrou teórica e praticamente que uma pessoa não autorizada tendo apenas um limitado material de informação com o qual possa trabalhar (e conhecimento de criptografia, naturalmente), pode extrair a mensagem original criptado por tecnica clássica, fazendo uso da velocidade, capacidade e habilidade computacional dos computadores.

Os métodos ou técnicas de decriptagem são tão extensos, ou talvez até mais, quanto as de criptagem.

Um estudo de decriptagem de fato abrange maiores detalhes e profundezas, o que não é o nosso caso em questão.

O aprofundamento em criptografia tem a seu dispor uma variedade de obras referidas, em bibliografia, de onde se destacam Cryptoanalisys e Code-breakers.

Este apresenta soluções ou quebra de códigos usadas na segunda guerra e na guerra da Coréia, além das tecnicas clássicas, enquanto o outro tem soluções de técnicas clássicas.

Tab.(4)

Método clássico	Solução (DECRIPTAGEM)
Transposição regular	Método de Givierge
Transposição irregular	Fatoração, Diagrama Triagrama, Anagrama Múltiplo
Substituição simples	Frequencia, Sequencias de Terminais, Contagem de Contactos, Solução por Vogais, Etc.
Substituição c/Alfab.Múltiplo (Vig - Gronsf. - Porta - Beauf)	Método de Kasiski, provável palavra, Etc.
Substituição c/Alf.M. - Autocodificação	Método de Bassiere
Substituição c/Alf.M. - Codif. com Nºs Periódicos	Método de Ohaver
Substituição c/Alf.M. - Polialfabeto	Diagonal, Formúla de Price

Tab.(4) Continuação.

Método clássico	Solução (DECRIPTAGEM)
Substituição c/Alf.M. - Poligrama	Provável Palavra, Met. de Hitt

VI. CONCLUSÃO

As técnicas que nós denominamos clássicas são realmente mais complexas na implementação de sistemas criptográficos.

A desvantagem desses métodos clássicos, é a de sempre trabalharmos com caracteres. Toda substituição é baseado em correspondencia de caracteres.

Desta forma devemos sempre, primeiro reconhecer o caráter para depois substituí-lo por um outro, de acordo com a chave.

Já os métodos que nós denominamos modernos, não se preocupa com o caráter, manuseando apenas com a sua representação codificada correspondente.

Os esquemas clássicos são também mais demorados na execução da transformação mensagem original-criptograma do que os esquemas modernos.

Isto se deve naturalmente ao fato das técnicas clássicas surgirem bem antes do advento da computação eletronica e da necessidade de aumentar o fator de trabalho.

Uma vez projetado um sistema criptográfico é preciso procurar aumentar a segurança e isso conseguimos de várias maneiras.

Primeiramente podemos trocar constantemente a chave e/ou o método.

É por essa razão que é extremamente importante que as chaves envolvidas nas operações sejam simples.

Em comunicações entre linhas a grande quantidade de informações é um "handicap" aos decriptadores.

Podemos então restringir o número de informações com a mesma chave, isto é, enviamos um "pacote" fixo de informações e em seguida trocamos a chave para enviar um outro "pacote", e assim sucessivamente mudamos a chave.

Com isso o parâmetro estatístico frequência estará assegurado a favor da segurança.

Um dos critérios no projeto de métodos criptográficos computacionais é aquele que nos permite desvincular o segredo dos métodos, mantendo somente secreto a chave criptográfica.

No entanto se mantivermos também o método secreto, ganharemos em segurança.

Um fato a considerar e de maior importância é a questão econômica dos critérios utilizados nas técnicas criptográficas. Em outras palavras, especial atenção deve ser devotada ao estabelecimento da exequibilidade econômica e operacional de transformações de segurança: a determinação dos casos aplicáveis de transformação e o estabelecimento de seus fatores de trabalho; o projeto de equipamento ou programas econômicos para a criptagem-decriptagem; e a determinação dos seus efeitos no tempo de processamento e requesitos de memória.

Existe uma questão real sôbre o preço que se deseja pagar por uma dada quantidade de segurança de informação.

Em alguns casos pode-se desejar todo um processador para implementar o sistema de contrôle total e segurança do arquivo.

Muitos usuários no entanto provavelmente quererão menor preço por menor segurança. Assim sendo a dupla preço-segurança é que indicará o mais adequado sistema que se quer projetar para cada caso.

As técnicas de criptografia em suma são uma arma para a segurança de dados confidenciais mas não a panacéia para a segurança do mesmo.

É preciso tomar outras medidas normais de segurança. Se assim não for feito, basta apenas roubar a chave criptográfica ou o método para quebrarmos todo um arquivo de dados confidenciais.

O uso constante das técnicas sugeridas dariam uma melhor avaliação das fraquezas e virtudes de cada método adotado.

Infelizmente a ausência, pelo menos no Brasil, de uso das técnicas criptográficas não nos permite melhor avaliar tais características, bem como os vários custos de tempo de processamento.

Existe, uma ausência, isto sim, total das técnicas propostas.

Em verdade muito ainda se tem para pesquisar no campo da

criptografia computacional.

Um campo para futuras pesquisas são os esquemas de matri - zes, como foi anteriormente explicado, somente que ao invés de esquemas puramente aritméticos poderiam se usar matrizes cujos elementos formam um grupo ou anel.

Acredita-se que pesquisas nessa área poderá indicar técni - cas de criptografia computacional mais econômicas.

Cremos que o trabalho desenvolvido até aqui já poderá dar um bom avanço na área até agora não utilizada nos meios computacionais onde haja informações confidenciais a serem manipuladas.

VII - ANEXOS

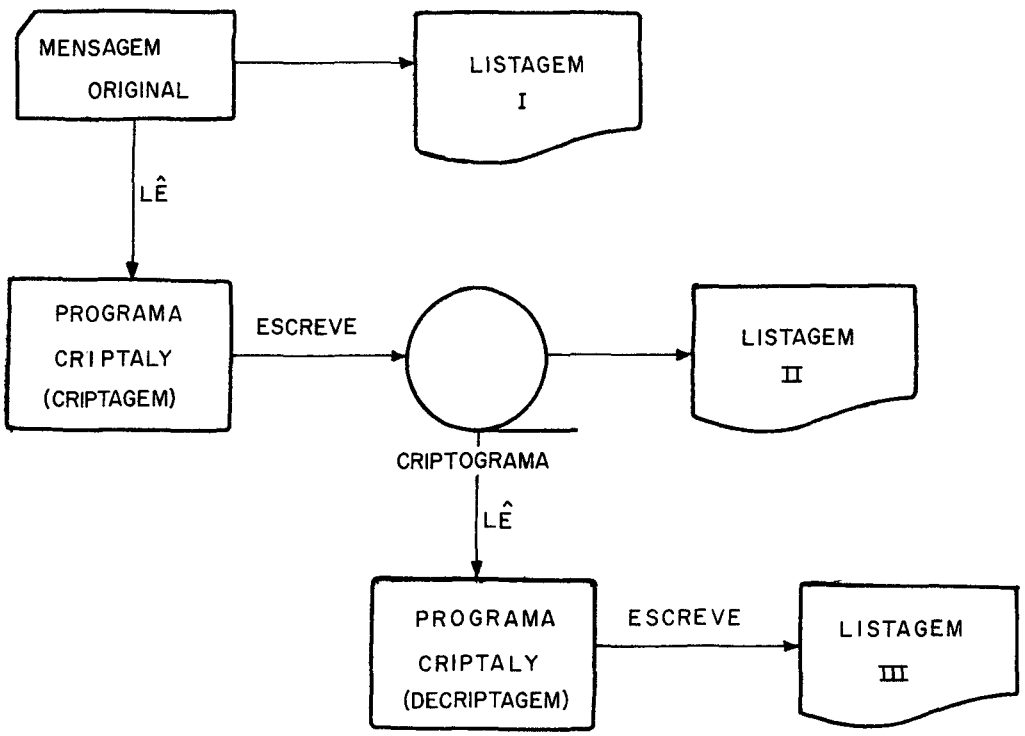
1 - Programa Exemplo de Criptagem-Decriptagem.

a) Com uso de método clássico (substituição de Vigenère e transposição colunar)

A mensagem original (LISTAGEM I) é criptado pelo programa CRIPTALY:

O criptograma é guardado em arquivo de fita (LISTAGEM II) e, posteriormente, o mesmo programa CRIPTALY faz a decriptagem, recuperando a mensagem original (LISTAGEM III).

ESQUEMA:



```
// JOB CRIPTALY
// ASSGN SYS005,X'283'
// OPTION LINK
// EXEC FFORTRAN
```

```
      IMPLICIT INTEGER (A-Z)
      DIMENSION INPUT(80),CHAVE1(1),CHAVE3(80)
      COMMON MAT(20,80),CHAVE2(80),ALFAB(64)
      DATA MX,MY/1,8/
      DATA Z/1/
      NULO=49
C     ****                                                    ****
C     * MX=LEITORA DE CARTOES,MY=LEITORA DE CARTOES OU FITA*
C     ****                                                    ****
C
      MASK=1
C
C     FITAS DE TRABALHO
      REWIND 8
C     ****                                                    ****
C     *LEITURA DO ALFABETO(COM NCAR CARACTERES)-CHAVE1          *
C     *      (SUBST.)-CHAVE2(TRANSP)                           *
C     ****                                                    ****
      READ(MX,10) NCAR,(ALFAB(I),I=1,NCAR)
      READ(MX,5 ) NCH1,(CHAVE1(I),I=1,NCH1)
C     NESTE PROG. A CHAVE1 E GERADA POR UMA ROT.DE NUM ALEAT
C     DE ZERO A NUM DE CARACT DO ALFABETO MENOS UM
C
10    FORMAT(I4,76A1)
 5    FORMAT(I4,A4)
      READ(MX,13)(CHAVE3(I),I=1,80)
13    FORMAT(80I1)
C     ****                                                    ****
C     *ROTINA QUE CONTROI A POSICAO DAS COLUNAS ALEATORIA- *
C     *MENTE                                                  *
C     ****                                                    ****
      II=1
      DO 16 J1=1,10
      J2=J1-1
      DO 16 KK=1,80
      IF(CHAVE3(KK).NE.J2) GOTO 16
      CHAVE2(KK)=II
      II=II+1
 16   CONTINUE
C     PARA PROGRAMA DE CRIPTAGEM PROG=1 E PARA DECRIPTAGEM
C     PROG=-1
C
      READ(MX,18) PROG
18    FORMAT(I2)
C
C     ***                                                   ***
C     * LEITURA DA INFORMACAO  ORIGINAL OU CRIPTOGRAMA E *
C     * / EXECUCAO DA SUBSTITUICAO  E TRANSPOSICAO /OU   *
C     *     /DECRIPTAGEM/                                   *
```

```
C     ***                                                    ***
C
C     INICIALIZACAO DAS VARIAVEIS I KK C L
      C=1
      L=1
      KK=1
      I=1
      R=0
      K5=0
C     SE E CRIPTAGEM DESVIO
      IF(PROG.EQ.1)GOTO 600
C   ***DECRIPTAGEM***
2800  READ(MY,19,END=1000) (INPUT(N),N=1,80)
      DO 50 K=1,4
      DO 60 L=1,20
      J=L+20*(K-1)
60    MAT(L,CHAVE2(I))=INPUT(J)
50    I=I+1
      IF(I.NE.81)GOTO 2800
2003  R=R+1
      DO 2002 S=1,80
2002  INPUT(S)=MAT(R,S)
      GOTO 2000
2001  IF(K5.NE.45)GOTO 7777
      K5=0
7777  IF(INPUT(1)+1.EQ.INPUT(2)+1.AND.INPUT(2)+1.EQ.INPUT(80
     *)+1.AND.
     *INPUT(80)+1.EQ.NULO)GOTO 1000
      IF(Z.NE.1)GOTO 4500
      WRITE(3,4501)
4501  FORMAT(1H1///40X,43('*')/40X,'*  LISTAGEM III- MENSAG'
     *,'EM RECUPERADA       *'/40X,43('*')/////)
4500  WRITE(3,2070) (ALFAB(INPUT(II)+1) ,II=1,80)
2070  FORMAT(30X,60A1/30X,20A1)
      Z=Z+1
      IF(Z.EQ.23)Z=1
      K5=K5+1
      IF(R.NE.20) GOTO 2003
      I=1
      R=0
      GOTO 2800
600   READ (MX,19,END=501) (INPUT(N),N=1,80)
19    FORMAT(80A1)
2000  DO 40 I1=1,80
      DO 30 J1=1,NCAR
      IF(INPUT(I1).EQ.ALFAB(J1)) GOTO 20
30    CONTINUE
20    INPUT(I1)=J1-1
C     SUBROUTINA GERADORA DE NUMERO ALEATORIOS INTEIROS
```

```
      CALL RAMBE(CHAVE1(KK),NUMRAN,MASK)
      CHAVE=(MOD(NUMRAN,NCAR  ))
      INPUT(I1)=MOD(INPUT(I1)+CHAVE      *PROG,NCAR)
      IF(INPUT(I1).LT.0) INPUT(I1)=INPUT(I1)+NCAR
40    CONTINUE
      IF(PROG.EQ.-1)GOTO 2001
C
C  ***CRIPTAGEM***
C     FOI COLOCADO A VAR  C APENAS P/ PODER MUDAR POST/ O TA
      DO 90 K=1,80
      MAT(L,C)=INPUT(K)+1
      C=C+1
      IF(C.LE.80)GOTO 90
      C=1
      L=L+1
      IF(L.LE.20)GOTO 90
      CALL GRAVA1
      L=1
90    CONTINUE
      GOTO 600
501   IF(C.EQ.1.AND.L.EQ.1) GOTO 1000
      NUL=NULO-1
      DO 101 LIN=L,20
      DO 101 Q=1,80
      CALL RAMBE(CHAVE1(KK),NUMRAN,MASK)
      CHAVE=MOD(NUMRAN,NCAR)
      INPUT(Q)=MOD(NUL+CHAVE,NCAR)
101   MAT(LIN,Q)=INPUT(Q)+1
      CALL GRAVA1
      WRITE(3,1005)
1005  FORMAT(1X,'FIM')
      END FILE 8
      REWIND 8
1000  STOP
      END
```

```
      SUBROUTINE  GRAVA1
      IMPLICIT INTEGER (A-Z)
      COMMON MAT(20,80),CHAVE2(80),ALFAB(64)
      I=1
      N=4
      DO 10 J=1,20
      WRITE(8,15   ) ((ALFAB(MAT(K,CHAVE2(L))),K=1,20),L=I,N)
      I=N+1
   10 N=I+3
15    FORMAT(80A1)
      RETURN
      END
```

```
      SUBROUTINE RAMBE (IX,NUMRAN,MASK)
               IF(MASK.EQ.0) GOTO 40
               IX=IABS(IX)
      IX=MOD(IX,666)
40    IY=IX*65539
      IF(IY) 5,6,6
5     IY=IY+2147483647+1
6     NUMRAN=IY
      IX=IY
      MASK=0
      RETURN
      END
```

b) Com uso de método moderno (esquema lógico)

A mesma mensagem original (LISTAGEM I) sofre o processo de criptagem pelo programa CRIPTOMOD.

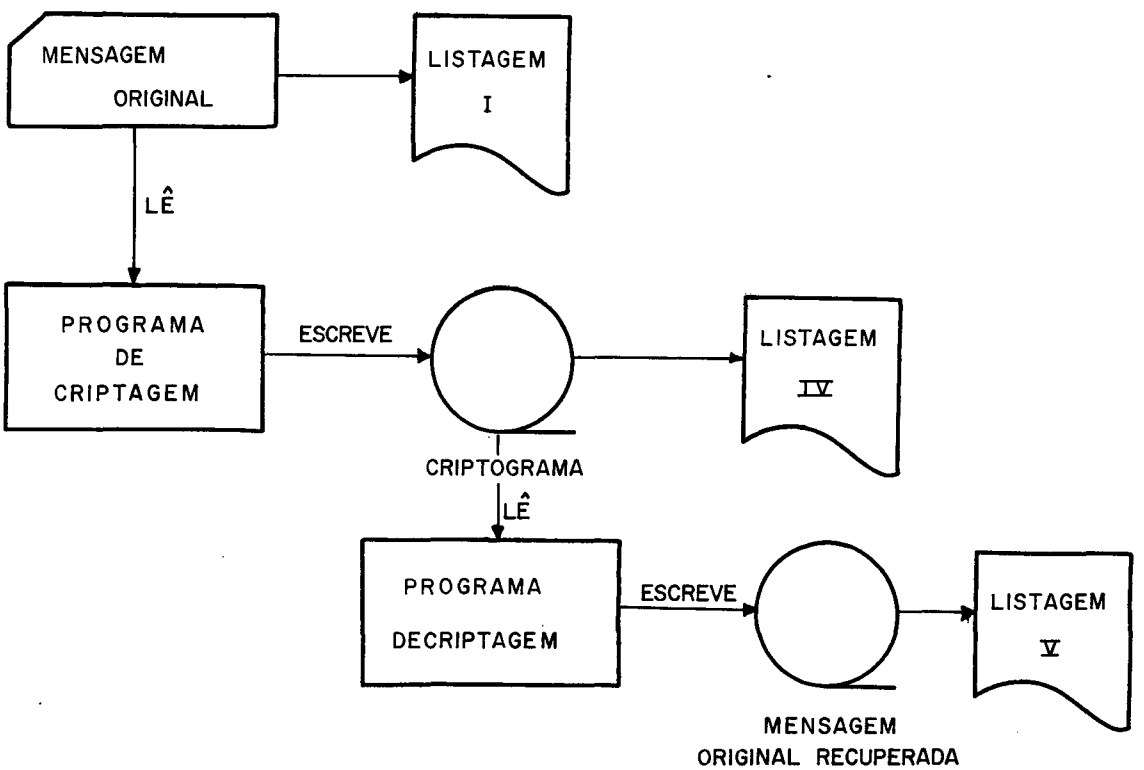
O criptograma é armazenado em arquivo de fita (LISTAGEM IV).

A decriptagem feita pelo mesmo programa aparece na LISTAGEM V, recuperando a mensagem original.

CHAVE UTILIZADA : YATO

MÉTODO : ESQUEMA LÓGICO

ESQUEMA:



```
// JCB CRIPTMOC
// CPTICN LINK
// ASSGN SYS006,X'283'
// LXEC FFCRTRAN
```

```
C
C
C      ****                                          ****
C      * PROGRAMA-CRIPTOGRAFIA  ESQUEMA LOGICO *
C      ****                                          ****
C
       DIMENSION INPUT(20)
       INTEGER CHAVE
       READ(1,10) CHAVE
10     FORMAT(A4)
       MASK=1
C      PROGRAMA CRIPTAGEM
777    READ(1,111,END=500)(INPUT(I),I=1,20)
111    FORMAT(20A4)
C
            DO 12 J=1,20
            CALL RAMBE(CHAVE,NUMRAN,MASK)
            K=INPUT(J)
12          INPUT(J)=IOR(NUMRAN,K)
C      ESCRITA EM FITA - REG DE 80 BYTES
        WRITE(9     )(INPUT(I),I=1,20)
       GOTO 777
500    WRITE(3,1051)
1051   FORMAT(1X,'FIM')
          END FILE 9
       REWIND 9
       STOP
       END
```

```
      SUBROUTINE RAMBE (IX,NUMRAN,MASK)
                IF(MASK.EQ.0) GOTO 40
                IX=IABS(IX)
      IX=MOD(IX,666)
40    IY=IX*899
      IF(IY) 5,6,6
5     IY=IY+2147483647+1
6     NUMRAN=IY
      IX=IY
      MASK=0
      RETURN
      END
```

```
// EXEC ASSEMBLY
```

```
IOR      CSECT
         USING IOR,2
         SAVE  (2,4)
         LR     2,15      CARREGA A BASE
         LR     3,1       ENDERECO DA TABELA DE ARGUMENTOS
         L      3,4(0,3)  ENDERECO DO  SEGUNDO ARG.
         L      4,0(0,3)  VALOR DO SEGUNDO ARG.
         L      3,0(0,1)  ENDERECO DO PRIMEIRO ARG.
         X      4,0(0,3)  OPERACAO DE OR-EXCLUSIVO
         LR     0,4       CARREGA  O  RESULTADO NO REGIS
         RETURN (2,4)
         END
```

```
// JOB DESCRIPT
// OPTION LINK
// ASSGN SYS006,X'282'
// ASSGN SYS005,X'283'
// EXEC FFORTRAN
```

```
C      ****                                              ****
C      * PROGRAMA-CRIPTOGRAFIA  ESQUEMA LOGICO *
C      ****                                              ****
C
       DIMENSION INPUT(20)
       INTEGER CHAVE
       READ(1,10) CHAVE
10     FORMAT(A4)
       MASK=1
C      PROGRAMA DECRIPTAGEM
777      READ (8,   END=500) (INPUT(I),I=1,20)
            DO 12 J=1,20
            CALL RAMBE(CHAVE,NUMRAN,MASK)
            K=INPUT(J)
12          INPUT(J)=IOR(NUMRAN,K)
         WRITE(9,111)(INPUT(I),I=1,20)
111    FORMAT(20A4)
       GOTO 777
500    WRITE(3,1051)
1051   FORMAT(1X,'FIM')
          END FILE 9
       STOP
       END
```

```
      SUBROUTINE RAMBE (IX,NUMRAN,MASK)
                IF(MASK.EQ.C) GOTO 40
                IX=IABS(IX)
      IX=MOD(IX,666)
40    IY=IX*899
      IF(IY) 5,6,6
5     IY=IY+2147483647+1
6     NUMRAN=IY
      IX=IY
      MASK=0
      RETURN
      END
```

```
// EXEC ASSEMBLY
```

```
ICR      CSECT
         USING ICR,2
         SAVE  (2,4)
         LR     2,15      CARREGA A BASE
         LR     3,1       ENDERECO DA TABELA DE ARGUMENTOS
         L      3,4(0,3)  ENDERECO DO  SEGUNDO ARG.
         L      4,0(0,3)  VALOR DO SEGUNDO ARG.
         L      3,0(0,1)  ENDERECO DO PRIMEIRO ARG.
         X      4,0(0,3)  OPERACAO DE OR-EXCLUSIVO
         LR     0,4       CARREGA  O  RESULTADO NO REGIS
         RETURN (2,4)
         END
```

2 - Listagens da Mensagem Original e Criptogramas.

```
*******************************************
*      LISTAGEM I - MENSAGUEM ORIGINAL     *
*******************************************
```

```
C      ****                        ******

C      * CONJUNTO DE CARTOES TESTES *

C      ****                        ******

C

       SUPONHAMOS QUE ESTE SEJA UM PROGRAMA DE GRANDE VALOR E
 ESTRITAMENTE CONFI-
DENCIAL.ESTE METODO DE CRIPTOGRAFIA UTILIZA TECNICAS CLASSIC
AS.
       PRIMEIRAMENTE FOI DEFINIDO O ALFABETO COM O QUAL TRABA
LHAMOS.ESTE ALFABETO
E OS CARACTERES DO FORTRAN(A-Z,0-9,E OS CARACTERES ESPECIAIS
 $/+-*.,()='& E O
BRANCO).

OBS1     METODO DE SUBSTITUICAO UTILIZADO= SUBST.COM ALFAB.MU
LT (VIGENERE)
OBS2     METODO DE TRANSPOSICAO UTILIZADO= TRANP.COLUNAR (MAT
RIZ 80COLS POR 20LN)
OBS3     CHAVE1 DEFINE AS REGRAS DA SUBSTITUICAO (LINHA DA MA
TRIZ DE VIGENERE).
OBS4     FOI UTILIZADO SOMENTE UMA CHAVE1 ,ENTRADA DE UMA ROT
INA DE NUMEROS ALEA-
         TORIOS.DIVIDIMOS TAIS NUMS ALEATS.POR 49 E TOMAMOS O
 RESTO(MODULO 49).
         ASSIM SIMULAMOS A CHAVE DO PROCESSO ORIGINAL (VIG) E
 TORNAMOS O SISTEMA
         MAIS SEGURO.O ALFABETO JA ESTA EMBARALHADO P/MAIOR S
EGURANCA
OBS5     A CHAVE2 E NUMERICA.PODERIAMOS FAZE-LA ALFABETICA ,E
XEMPLIFICANDO=
         CHAVE2=  METROPOLE

         NUMERO ASSOCIADO A CHAVE METROPOLE

         METROPOLE

         319857642   NOTE QUE A LETRA O MAIS A ESQUERDA TEM V
ALOR CORRESPONDENTE
                     MENOR.
```

```
          ******************************************
          *     LISTAGEM I - MENSAGUEM ORIGINAL     *
          ******************************************



        NO ENTANTO FOI FEITA UMA ROTINA QUE LE OS NUMEROS NO
 FORMATO I1 (80NUMS)
        E SUBSTITUI AQUELES REPETIDOS,BEM COMO SUBSTITUI OS
 ZEROS DE TAL FORMA
        QUE O RESULTADO E UM VETOR  CHAVE2(I),I=1,80 COM VAL
ORES DE 1 A 80 DIST-
        RIBUIDOS ALEATORIAMENTE.

OBS.FINAL= ESTE FOI UM EXEMPLO DE CRIPTAGEM E DECRIPTAGEM BE
M COMO O PROGRAMA
           E UM EXEMPLO.COISAS MAIS SOFISTICADAS PODERAO SER
 FEITAS.
   O QUE VEM A SEGUIR E UM  PROGRAMA CONFIDENCIAL (OU ERA...
) QUALQUER EM FORTRA
  N

*

*

*

CONFIDENCIAL       ************************************

CONFIDENCIAL       *                                  *

CONFIDENCIAL       *  PROGRAMA FORTRAN CONFIDENCIAL   *

CONFIDENCIAL       *                                  *

CONFIDENCIAL       ************************************

      INTEGER A(8),IPUNCH(10),B  ,P(10),PUNC(10),N (8)

      DATA IPUNCH,B/'0','1','2','3','4','5','6','7','8','9',
' '/
C

C     LEITURA DOS CARACTERES ALFABETICOS A PERFURAR (A),N=NU
M DE CARTOES
C     ,A-ESCRITO NAS 8 PRIMEIRA COLUNAS E N-NAS 8 COLUNAS SE
GUINTES
C
```

```
**********************************************
*      LISTAGEM I - MENSAGUEM ORIGINAL       *
**********************************************



      READ(1,1) A,NV
    1 FORMAT (8A1,I7)
      K=8
      DO 2 J=1,8
      IF(A(J).EQ.B) GOTO 3
      P(J)=A(J)
    2 K=K-1
    3 IF(K.EQ.0) GOTO 100
      DO 15 IK=1,K
   15 NK=NK+9*10**(IK-1)
      IF(NV.GT.NK) GOTO 100
C     ZERAR O VETOR PUNC -PRIMEIRO CARTAO PERFURADO=..ALFAB.
.000...
      DO 4 L=1,K
    4 PUNC(L)=IPUNCH(1)
      K2=8-K
C
      PAUSE 'FAVOR COLOCAR OS CARTOES NA   PERFURADORA DE CA
RTOES'
      PUNCH 6,(P(I),I=1,K2),(PUNC(I),I=1,K)
    6 FORMAT (72X,8A1)
      NV=NV-1
      DO 7 NA=1,NV
      IA=0
```

```
*********************************************
*      LISTAGEM I - MENSAGUEM ORIGINAL      *
*********************************************
```

```
      DO 8 J=1,K
    8 N(J)=MOD(NA,10**J)
      IF(N(1).NE.0) GOTO 10
      DO 9 J=1,K
      IF(N(J).NE.0)GOTO 9
      IA=IA+1
    9 CONTINUE
      GOTO(20,30,40,50,60,70),IA
   70 IC=NA/10**6
      IF(IC.GT.9) GOTO 100
      PUNC(K-6)=IPUNCH(IC+1)
   60      ID=MOD((NA/10**5),10)
      PUNC(K-5)=IPUNCH(ID+1)
   50      IE=MOD((NA/10**4),10)
      PUNC(K-4)=IPUNCH(IE+1)
   40      IG=MOD((NA/10**3),10)
      PUNC(K-3)=IPUNCH(IG+1)
   30      IH=MOD((NA/100),10)
      PUNC(K-2)=IPUNCH(IH+1)
   20      IJ=MOD((NA/10),10)
      PUNC(K-1)=IPUNCH(IJ+1)
   10 PUNC(K)=IPUNCH(N(1)+1)
```

****
* LISTAGEM I - MENSAGUEM ORIGINAL *
****

```
C
      PUNCH 6,(P(I),I=1,K2),(PUNC(I),I=1,K)
C
    7 CONTINUE
C
  100 WRITE(3,101)
  101 FORMAT(1X,'ACABOU,OU DEVE HAVER PELO MENOS UM CARACTER
 ALFABETICO
     *PARA SER PERFURADO,OU HA MAIS DO QUE O NUM.PERMITIDO D
E CARTOES')
      STOP
      END
********** ESTE E O FIM DO EXEMPLO DE CRIPTAGEM E DECRIPTAGE
M ******************
```

```
*****************************************
*        LISTAGEM II - CRIPTOGRAMA      *
*****************************************
```

```
U5$S(JHMW=A)MTSOM()&+I,JW9PZNY1/2OZV/OAJ AO$J-NLL(6JY)+8L&54
(AJD8W8E6B5D$5HRG&8F
IVG89$5-LND7IIT,ZRP/*UL7'TSZ+JCU&O(B(3ZZK9++,)OQ5.$TU(,I1,9Z
)6-P8OBC*QIB)$B.(BN8
4,ZU*43TWAI8B17Z'IDP4J1=UTOV4XQU XAQ&YBC(P&6,DK.-7*RTJP1Z'PG
2FM--$S*7JAQCDQ**AVJ
C1KP3SLB=)FMGT3,2 6-D,4,X+YVWZXOU&-4M'CID.VX))''TRF877,D.A-O
3VI$LJ8IM1)E '5 MFCR
NX8S&G( -5HG*TW=VXK$ ==PEE(NH31A'25&MSVZVKBVD9JM24')SNM+FD9-
N955+'2M/EN1O+*NRO8O
A8X4(TZ1CV'/6*WXC9Q891025R/QJ,)N3.$)GEJ97X'Q3B$AH5IMQOU6XO=A
U$ZUZP /DBVK'=95AEW$
YK.)*RSC1X6L.B)9S.$D2&/AWF(HK)=ZK('MX-V=G7I9E-/BQ5(O,SS=EBT&
B1*4-HQ=ONAL82X$L4(Z
4GZRGD)PO )6QPN'VIWM(DG)&7&CZ=RC*WHAMNNS)(3XO(OVOMQWG1VB4JD8
KDHQDZI=JY6$*=8W)HIA
2RGFUGDK7)U1=W=J9T=OK8EOYO$+YD9'I-'+NTF$M18 7CDF.,.WIYJG(701
O5S(2ZI8/C. RU5RIERS
'&P/6YM/A36 ,OQPC)T6.DD.+ Q/R7UVQB98=Z-U9EDZY7VHF9$FZ=(X*5HO
DQC3JVO5T/Z&N(43T(F&
X8 H$QR3QI4.(/19UPIUJB93L7/OH3V-,TS+I746KW(WPNWUQ*,M7W(G/P/P
.N71D-KAR)FSA( JH(7)
/',IXVS1DX*/G'-OTQN.W1K//H$9G9OTXN$(G),1)N(YB7KK*-K9BH(Z4'SI
A/E)Y'/+NAP4/=6IHV/(
*E4*3Y H)I.2K2Y&9.9+IG52+.XKZ4IZ1SU'**ZA)7Z $1TKU1 D=/XJR9WL
LL489N+64,4G3,.MIB=N
M&XC- 3A-  $J1(M,9/US,X+,RK3M*TI113YRO1=-5X)-QO6V$KH&GNNRO+7
3$+X)ZKWWR'A /R6EL6*
L4 1Y$HIH, DXI47H-'+CMIDS35&Q$.AYD+K1L((3D(1*1L15ITLOXVO()&,
OTBOVXS9Y/&9CO28ZPTA
H8SOZ 204VRUAYO)W-Z4HZ.B8373N6RSEO5D=5OA9I9=MVH8GLUWPPXIQ6 U
/TV8S1*5CTGZ.6+O+V'O
H(N=8C,AV96GVR&SG1LK73 /N2N5&(*L3XC*B2FAR*J3'(NOP61 5F22A92O
EG2FL4IF( 9WKB&LNOJY
T*9/,CTP'J, OE8(ZFOW8*T/WWFALYVO7Q/MFUG$W273,X$NIZO'IQ*7J,6V
U2(D2.S&S'J Y8URA/U'
XOE).3QEUJ.'YWR3GSJW='AHF4/)82'/71(8,35'+,HS=F1&J75&-ZEOR'Z(
3W*W9+VQ5I3FRE*XONO'
&9JF+/S&VKM2.O4B1MBPQ$14/IFSJE4V,RL78WXUOVWG1USC/D=Q 'T$3$K*
 3D3C62RBXBS2(PAVW$O
P-PC/X-INV,+)SV(QG/$9D),5/CC43G(EN9X4BRHOXF47I5-RYT2H7IXZ3Z=
..BI* 4)WGF$33.B'G)7
K ./GN).CLOV,6PBYEOODDDJAKS IZUN(96NCG/M)(HEK(OJ4P&MTW9NW-UF
HN''C)7O5H67NQ=9UKIO
```

```
*********************************************
*         LISTAGEM II - CRIPTOGRAMA         *
*********************************************
```

```
CM FCA+90X3 F=55YL)I/PD*L25+G9TY-=9)UB,JYON'L6TS3H  XOYQL TS
FI-WGPCY L.,4YY=OK2X
C)5&S8.*1SMC89VSO7'82CM3CS7LKO O( (UJ8,FG$E/.RW,6=,*6LQ$EV*C
TO/OQ$*OP5S-RR)R.24J
YH+&+UA-QX*BERJGIGLFTI8GO1Q) RE)U+LEK(&AP+5ZBX)(4*+,.WW*WIL-
'JC3+2(NBSOJ6O5)(P4=
= T4 X*HQBHOY/ CVO(DDLQ7UA82UI*IC$,AIPV(-/4V&)5H(2+ MK+XJ7LJ
$TAA1'NE$Y8W8+,K= *-
-.T&2PRRBO-.9LQE7YAO5=ZU*4 U+=*Y+.')6PP1/5XO1PSG728MTG=XMK*9
Y(UD 4H'-O.1)6,HWWF&
4/6ZKFESBH5YIV$5QS2OC9TJSB5P(Y3 ESHTBOLFL+K (DF3'5/)Y*L,&YZC
CA)D19Y9)L)($GOD5T)+
+V1YAIM)-W)3=(BJYULLOJJO3QGKSR557&RW,KTGLM.6UXS3BON9TJ7I,4KY
$31U =,$)S961MTD4HHR
L1O/3AF)/+OG*W9DHP3DF,ODG+XN5I1OF$ O5 &TI2&RXRK3*W.K4MZOC-RS
W8*,RHSFBDZ(ZH4-4 2P
M2M+(H+ME HQ$63RZOGKV2AFMJ4PBMVK58GF.,*.79FDK2ASI-W/BLYO)H2W
GBFTBW*ITO4ETJGOR/Q/
$G9JYMJEH5&H-F8S/DOF.JY+'O2+O(2Q-KUTEE9,XSGJLV&N.2.I-M85QR4V
(R26=642XUI9(Q,J1/ +
(14'OOUP,-15' 1$7O9D496&'6&K79EN1PBVCP29BAOD-+I'H'3 X*QO/BEP
G'MOG ,,,L+D1(1',/&&
BAKFLN9+O1U9S=X7=EJ+K-D1=WQCH5H*1,R1&I18NH$4'JFF99. K4B5OZUB
M(NVCDW-9MR&++(K65FS
*OHN *I$1A7)K42NVTHW1- W1-(YB-.L'6'WN*'DVF43ER6MG7L1S*K3/LO+
CL2H.TWOLPH=VGH7C&.W
8KH-8NU)H2O'M/25XRPKI2.,GSE1QZN8+QU-'YWJ5ZOEXUBU-SZHOQG1WX5Z
R-9=8$ZX-X3,OX 7TJH/
8F16N5HFQCRH4P5D(2-'QUCRT9H,+()7W4IQ)SFDW4JN,A3QB 7I93'QE2SF
D-H+2F5D5Z,AAUX*YIN,
Y*JLTI($O+X1&YFNZRPOMUU2X6/VX/PBM+WP4RR.&/ 1=$4(HOGG3=)$OQW9
E/5'E82FBV+Y82+MS2J.
''1IP6XC1IZ2J6*G8V4GLONG5T= -C+=B.=&4U26JCQC86(BQX*4$,KVRRE6
WY=-'8CT/3DP3R,*YEBS
AW4G/$O4H2-PYL+(.'4 3KD1V9Q(ZGF'M&W)5*&$KY$T+S),YFWJFVS/HZ4S
N$&IJH,1XH3EG1CW+UZD
JOYY+11GUHTA.MM/)PU9CCDLUN.=ODTK*A5DMZORSCVFQYD+B1()R$(())FU
71E&E6TECT$MDF)U4D8P
 T'$QU4(V52R-B'Y*ZA'Y&YVPJ*GL'P4+26UWG)4Q&P-S+*C-)3VB.5*O)*C
-,HS6MWR5UE9Z(T H*/U
'WAOWB,M25$I*L,G.RBOEXZ=P2+6V4 ZPG'N=K5BCHA(C1.9GN=93SN-QI9-
U2 *,',QFVEO$UQ,9$F&
X$2I=1JOO$P*O-5B1/&,$V'APEVGY4FGZYA(9OG91CPZLJU8*+-CF(MCQ1*/
CTQO3K/5/FG'MIIZF2=3
```

```
*******************************************
*         LISTAGEM II - CRIPTOGRAMA       *
*******************************************
```

```
(FAMJCZ.'88L&*/8$5(SV*BW6F90/ 8PY=HH62TCCN*$EL)QR9IK*XOVMXD1
(PKUJJ+MVIOZYIU8XL +
J)YC F2ZLH3ME/&HOME 6=$OOKFJ-58= ,1LP6-PU8UARTM & W,XP3HR$DK
VBH+JS*T 9W$,,UNR$AX
95OEFMUB,6MNV.3DO96 R33ULK YJ*5$BX'152Y(6F9Y*M&'5T2B-'GEP,6D
FDXL G-JOYC/1B/JU/X/
K$Z 76DY2/+A9 *T)*AV-/=P*WA& ,2J4A-(LT69-4D3HKJ58,9D3U$=3&JX
R8T'OE2KTLSGPWQSFY59
XVHC3MFM)H1T/PYDC5JGVJ*G75NO)SMP& 7X7'.3L&PO*BN-+H6'J30$NSDJ
)840UKN5TIL'WQ&H&18K
X-YLQEI3/OQ9RS(=BF'1CB*ZNVVVIW6.LLG-BY-U, PNJ+I,P3+YH1LB/$W2
 ),JJO1JCCQDUOLXTBLT
L6RAOC*+24*J(-36PY)F'P3*J='AA').B5TDA$YHJDMI/U(XCQJ7Z$/QH)*Y
OV'C(8MCD4,=KL1//HQM
JEO+Y4SY,OEH 7+=-OZW)G)N57W/KO/FLU7PP-/-73QGQ.84/TCS7FD ND)C
&C,X+=W23'7)7(NZ)Y7(
Q3O2XNNQ$4-H*FO=&7'YBKDD1PHGFLHQVWDA&/QQ=C,+33IB29H=9G+5/=.(
3BP2H*.=X,,W5(V+89AH
( 6E4V Z-1SMC5TU.V7MH3 *1P=BUT)7$Z)-=$A&W()3GFP1$D/NC44U,)XO
RBO&FE1Z2+9SO5P&*'QU
HCQJKON&QI-&&WQCBKTSC=OFI-Q2NI4=RA3MBO.R*ZR8X&J,U 'J B..S&W'
ICTQZSSN/LG$XM-FSD7H
XZ=N /RFQZH&7+,UU6Y7=8C/74*KU($$-8U76C+E-L&R8S42+6RJL$80$D8-
AC$L4LZS'AYGOI5G)W(O
3TWCA3474ECTDI4EOGYV26ZYL*YO6&RR/(VDQU1+O)IXGQZ56K/ Z*YG.*KN
7$JO/N(2=MV&MQW'.&V3
I2LNT=C84$G8CE2JOS*5*&VU&JK=(F*=ORK'M7CI6AKVNO75O+(S)'/1=J(W
14YBZO5O'64O+&OVY(D6
YO2/E3W'8$OPPCOXH*O/W*MPSO KNO2-P=AUS8ACFUV4O5,FOM=YP$3ZBPYG
L61RS (E5& 9IMSEAOP.
155I+U$WF3EUOQ),.3DUB6=A2G=-KS9Q'OENH95543W*L8M)B.J29F8$G1*
&WXI1.JRPSEBOV.=OPK.
P61)&&L),OHXM1N3F4TY44AL8'CTY'-/,BPI4 /I8CNJUUB.SN8N =(XG&BA
.BTO7&+PZ6A*K.O6R,IJ
=DSOMT8VE=29+ZS2H75=FOWRWE//89EG'FP+KF*.YN$WICP7LKG29G=)+FPB
9MO N4C4M4&'4 6'2RY9
'(&G-Y7U*C5/CVVNG8JE'O7('KPHZV(WP+ .*23)4JPOAH3EQB6H4QV7S2/9
F,+EDT+7$O//H1WO 42G
FSLO)69&1&C3=HKOG PM7)898SWTKL=FHM'&,X=*N/.Q- 3M96QR1.A=B3U$
$GV,1VONJCZRP-/57SJ6
 SJCQLD LM(P-QV(2*4YK 8 7N3R&R)Z3TGRRZ/H*5-KVO$38''IVI4NJ 6'
Y9I,.H.-ILFJ$+68&KL)
 I'XRY1)1DQCSZ.VO4(Y2UBO-,13CX(D48'B2N$$S=WBDUAWHN UW5SS,6*D
(PO).=BAI,E=7W-4 IKS
```

```
*****************************************
*        LISTAGEM II - CRIPTOGRAMA      *
*****************************************
```

```
.)NO3M4UZRZM(7Q+1OGXF+T84,'RL(5'5.9DQY(1LNB*BILPH-E/3*F/RKQ.
R8,,5B2WPW2WRS88*81+
V+/KI(JU)PN,RPL3Q(UG ,4L9A26 /DYYN1M-8A87DUOJOS-F7+)=Z 3V3UJ
457-'CGB+'/ 8G1'Y-5N
CG/*6ON)QBS+AP.37O4KOHP 9'=-XX+N/Q +O4ZM/WFZ5ICH.88)/TUQY$'3
PW1VZ+C D,R.DPOQ=MOQ
4)UJ'E+OB'IYM$5*18)D&P4C(L2.(6C(Y21(ON/DRRO.UUR')KO)POQX$7Q5
C&2QQ,OE*JE8SBAGRYCT
.OOHXFUM2W95RKTE=FOGDZ9A)U&LAVO&75*LTV56RLF6707OUJWQO*Z(+UB3
UICB6LSK=&KV.TLQII*T
PRW  87.L-=R-'57V(PLD9PWXO8R2UJYHS9U5IFDATHPK7XZ81O'8*2PR /&
IP*U8AMWCR/EMNY(UIUT
9/V8MQSHFSM'3&M6V*A*&4XGPC18,-,E8ZT2YU5A)22=Q1FAW9NNSXP5E,$Q
W,EJA/A*7Q4RNV1XTLQ,
BVGY7CD'$C/=*B5O1Z1RXRB3D')65U4T-1,SS-MV$3BNC).QAO*LXE&(*'C7
'4N*BLLUJFS9B$DXPT1H
$BGHOTPBKS6+)(5W*VJA=/*Y.L8(PTRB /O=OSX,S53Z1 6UCBVNXJ'KOF4N
JOKO&  9(+CU$O8$N2NV
L+E/OL+PGI*R)/FG F('S=DS-F4Z 1TV9OLL.Y9O - +RMXLN8X3+*POL*K7
HMY=X*+3)ROOLP &PE.I
=J==DX,116LG($4BV9P,WJ7 I*XS-6WX(-54'54N=1V8YJOOJYNU83JN45C9
C(F)8WB'OSOSYKLJAVX.
/6IV1PNK,*$HHN2-OE(B/G1*I3=9G9.1IHTB$)C(-6ODWMJFXSONZ44+$4(X
 3RLY35S71Z*.-C&9XBZ
Y3H&61FW9YOHOS5.R-2XJ$QVX2OQ3J&=X51(=C=H69X1CXP$KKCK/B-PWU54
$)8S5KQ,J8TJ.ROQZGC*
'HRX+FNRDF.-'C K)M/*XVZW71OO)7+&B$USQKDXREE)DL(1H,,M(2J+JF85
MXFNDYZCCN)'42+8 'AF
YL5C43O,*2OK.TR)HZB3OHHX(FDL)2QVQ79/+(4LQC+7IFML+IY+9+-2,U+$
IQD/5Q8QNZ+8CZDW ).6
LN8BM,546(L/I,/TS9O)HV,OYJS(Z=74VO7/6GB-/R*L2L1NH4HQA.DUFOBW
7)X9CF7XTE9TC=&8KNNL
9+4C&OFTOEFAUEOMDX883+WYH.W-RS7C*9 AF733K-(+XU8HZP59NGOGBHZZ
8)=(2R6UFJUDADMI4RD,
+Y9'('N+HI8 Q'8HH2-D7E=6LOU+51/CPJR+IDVLA*W2N25 ZX48YYE'7&DN
$/A$$COW/DU36..5YV,W
/COD,2JTKVK)M6R2O*C-3MK6MQYWA9==SOI$1LUDD57LO6MD6L XBXSIO$5O
=U8WJ4XSOI(7X78L6.ES
TL&-H$PA+GPVIL$$LEBX&CIW5IQ-CZ-WOXS9U2Y8.=+LM1E&PN/&,I(V6-JD
S15)C )USECF)1$M)-LJ
NUHFV$O+ADIGK/UMD,9YBMON/V7&R4Q6VSQ=P KN6-Z$$5N677N6.+)G-Z(=
VS3WF(OZ*NWKGQR*CVZ*
S4=/WC3MPP5ZPX-)H&7J8E+3KYOX$U=O6V*OX2R3RG=L5=/EO'JKE36NM2Q*
K/S5NSMD,,-TB7PT+&O=
```

```
*********************************************
*         LISTAGEM II - CRIPTOGRAMA         *
*********************************************
```

```
/J.19J4TYK/G' BDF0AVG37S39=8OTNO7IS44*CH*E9$E)42 V+T&I7UKW&W
3TJ1S(LM3HZ6*C3JNJZ+
9D$+LSS H//,FFTYV 4-G9AUE()EY47)'WAZ&VE*8WN*WR/.H(WP.Z7CZ-5$
YE146=FBBK13$*RINZ$T
G4J&2NX+*C8,ARM$$,S=/6(CZU-,$KF(BB3S3V$'&S*(ALJXO5++ I9BPVE)
HR8/GWY. CRVOJ)J4P.H
1U3GLNA97(M LC+DP(DGDMZEHP$NLYEBKVLWW -.4-TK*A,7,*KX=)OV XL5
-LVOHB**&6=B3ES(RU4G
&5 D98 (1/E1XB(RA1+5TB+-YM'49W.77=IIGRKU )T 5'RULA(Y&16XB'W+
VZH)$WQ5N&I &-T,2EM4
D$WF(-LW*=')7&2X8S1B*BB,02SEO1(E-KB& AF5T.V66ML5 9Y+5VD-RU-X
C9JS=',9&2GDJD=05RUX
F*E.LR$3X&OSCOQBPA32QDTSJ(UB8.CYUL8O-F/**+E=2TI)2+BLCS8XGDO+
&V,XD+W$P3N*'*15/18E
RK$HC-W==)Q)6NB,8'*4)GU(**B7S'C(B,PS+FKM(H$&DO 3 3L*29OSRKH,
A,ZLMDY,QTY-44&UR$)Q
HZ=86TL7*BA774*RC(6ON$D&J&5 IWSTA5$'2,.&81&AC.XVGSJXLXZ &X63
QU *41L8X$IW,W9CODKO
UZ(&4 P))04S89ZL)FXAR.=MZKJ'USJBESK5DOR2F= /C -Y2LTXF),-XLD&
QOE6=D1OJ-+MGCY(=+W*
W)FHUVV) R,FCX/ AJXBW1-Y3E5H=WZ1MJKMKZ8138'M$=1$5G(DW,Q/B7,N
L,N8H Q+5-9XJFI=II+N
T.L4YDRFSQ JX*+LU+E5/S CNZ8O&*I$)0279=ZP*9S2.9, UMNLB(9PQD-+
9X1Y7LICH,XZRDMP(MZJ
```

****
* LISTAGEM III- MENSAGEM RECUPERADA *
****

```
C      ****                    ******
C      * CONJUNTO DE CARTOES TESTES *
C      ****                    ******
C
```

SUPONHAMOS QUE ESTE SEJA UM PROGRAMA DE GRANDE VALOR E ESTRITAMENTE CONFI-
DENCIAL.ESTE METODO DE CRIPTOGRAFIA UTILIZA TECNICAS CLASSICAS.

PRIMEIRAMENTE FOI DEFINIDO O ALFABETO COM O QUAL TRABALHAMOS.ESTE ALFABETO
E OS CARACTERES DO FORTRAN(A-Z,0-9,E OS CARACTERES ESPECIAIS C/+-*.,()='& E O
BRANCO).

OBS1 METODO DE SUBSTITUICAO UTILIZADO= SUBST.COM ALFAB.MULT (VIGENERE)
OBS2 METODO DE TRANSPOSICAO UTILIZADO= TRANP.COLUNAR (MATRIZ 80COLS POR 20LN)
OBS3 CHAVE1 DEFINE AS REGRAS DA SUBSTITUICAO (LINHA DA MATRIZ DE VIGENERE).
OBS4 FOI UTILIZADO SOMENTE UMA CHAVE1 ,ENTRADA DE UMA ROTINA DE NUMEROS ALEA-
TORIOS.DIVIDIMOS TAIS NUMS ALEATS.POR 49 E TOMAMOS O RESTO(MODULO 49).
ASSIM SIMULAMOS A CHAVE DO PROCESSO ORIGINAL (VIG) E TORNAMOS O SISTEMA
MAIS SEGURO.O ALFABETO JA ESTA EMBARALHADO P/MAIOR SEGURANCA
OBS5 A CHAVE2 E NUMERICA.PODERIAMOS FAZE-LA ALFABETICA ,EXEMPLIFICANDO=
CHAVE2= METROPOLE

NUMERO ASSOCIADO A CHAVE METROPOLE

METROPOLE

319857642 NOTE QUE A LETRA O MAIS A ESQUERDA TEM VALOR CORRESPONDENTE
MENOR.

```
      ******************************************
      *  LISTAGEM III- MENSAGEM RECUPERADA     *
      ******************************************



       NO ENTANTO FOI FEITA UMA ROTINA QUE LE OS NUMEROS NO
 FORMATO I1 (80NUMS)
       E SUBSTITUI AQUELES REPETIDOS,BEM COMO SUBSTITUI OS
 ZEROS DE TAL FORMA
       QUE O RESULTADO E UM VETOR  CHAVE2(I),I=1,80 COM VAL
ORES DE 1 A 80 DIST-
       RIBUIDOS ALEATORIAMENTE.

OBS.FINAL= ESTE FOI UM EXEMPLO DE CRIPTAGEM E DECRIPTAGEM BE
M COMO O PROGRAMA
          E UM EXEMPLO.COISAS MAIS SOFISTICADAS PODERAO SER
 FEITAS.
  O QUE VEM A SEGUIR E UM  PROGRAMA CONFIDENCIAL (OU FRA...
) QUALQUER EM FORTRA
  N

*

*

*

CONFIDENCIAL      ************************************

CONFIDENCIAL      *                                  *

CONFIDENCIAL      *  PROGRAMA FORTRAN CONFIDENCIAL   *

CONFIDENCIAL      *                                  *

CONFIDENCIAL      ************************************

      INTEGER A(8),IPUNCH(10),B  ,P(10),PUNC(10),N (8)

      DATA IPUNCH,B/'0','1','2','3','4','5','6','7','8','9',
' '/
C

C     LEITURA DOS CARACTERES ALFABETICOS A PERFURAR (A),N=NU
M DE CARTOES
C     ,A-ESCRITO NAS 8 PRIMEIRA COLUNAS E N-NAS 8 COLUNAS SE
GUINTES
C
```

```
*********************************************
*  LISTAGEM III- MENSAGEM RECUPERADA        *
*********************************************



      READ(1,1) A,NV
    1 FORMAT (8A1,I7)
      K=8
      DO 2 J=1,8
      IF(A(J).EQ.B) GOTO 3
      P(J)=A(J)
    2 K=K-1
    3 IF(K.EQ.0) GOTO 100
      DO 15 IK=1,K
   15 NK=NK+9*10**(IK-1)
      IF(NV.GT.NK) GOTO 100
C     ZERAR O VETOR PUNC -PRIMEIRO CARTAO PERFURADO=..ALFAB.
..000...
      DO 4 L=1,K
    4 PUNC(L)=IPUNCH(1)
      K2=8-K
C
      PAUSE 'FAVOR COLOCAR OS CARTOES NA   PERFURADORA DE CA
RTOES'
      PUNCH 6,(P(I),I=1,K2),(PUNC(I),I=1,K)
    6 FORMAT (72X,8A1)
      NV=NV-1
      DO 7 NA=1,NV
      IA=0
```

```
      ********************************************
      *  LISTAGEM III- MENSAGEM RECUPERADA       *
      ********************************************


      DO 8 J=1,K
    8 N(J)=MOD(NA,10**J)
      IF(N(1).NE.0) GOTO 10
      DO 9 J=1,K
      IF(N(J).NE.0)GOTO 9
      IA=IA+1
    9 CONTINUE
      GOTO(20,30,40,50,60,70),IA
   70 IC=NA/10**6
      IF(IC.GT.9) GOTO 100
      PUNC(K-6)=IPUNCH(IC+1)
   60      ID=MOD((NA/10**5),10)
      PUNC(K-5)=IPUNCH(ID+1)
   50      IE=MOD((NA/10**4),10)
      PUNC(K-4)=IPUNCH(IE+1)
   40      IG=MOD((NA/10**3),10)
      PUNC(K-3)=IPUNCH(IG+1)
   30      IH=MOD((NA/100),10)
      PUNC(K-2)=IPUNCH(IH+1)
   20      IJ=MOD((NA/10),10)
      PUNC(K-1)=IPUNCH(IJ+1)
   10 PUNC(K)=IPUNCH(N(1)+1)
```

```
      ********************************************
      *  LISTAGEM III- MENSAGEM RECUPERADA       *
      ********************************************



C

      PUNCH 6,(P(I),I=1,K2),(PUNC(I),I=1,K)

C

    7 CONTINUE

C

  100 WRITE(3,101)

  101 FORMAT(1X,'ACABOU,OU DEVE HAVER PELO MENOS UM CARACTER
 ALFABETICO
     *PARA SER PERFURADO,OU HA MAIS DO QUE O NUM.PERMITIDO D
E CARTOES')
      STOP

      END

********** ESTE E O FIM DO EXEMPLO DE CRIPTAGEM E DECRIPTAGE
M ******************
```

****
* LISTAGEM IV - CRIPTOGRAMA *
****

```
CA&OC +<M(&CP>9&XLCCRXL&6ΔLO68;<M<B%3=U&Q)FO??C&3%ZOQ9E&4 ZO
"3D&N UOT 6&%/ΔO87'&
YA|O5<,&+" /*?VF7A?OOwJ3B1&OC.'3PO5%OZZ&-(NOKMH&= OOPO &O?YO
<'A&C*COCCC&4E,O2I &
 /6O DO<(6;C,.T& )AOU)(&OZAOMS&<Z_-%O.=&R'MOU E&|3XO/E"&9JPO
Zw+&/UBOCP&&  O+UX&
Z7(OBP1&RM_O5)&&X&HC+OS&5  OT I&<A3CI T&R.CO4|K&2++OH;4&V460
wC,&2ZROwCN&-+RO4DM&
%5MOS U4(C98:ZC2I;C5MOV3:5(5YDO4.;(ZA)AJHFS4.>YI+U/5ΔΔ8CQ+E5
)*:3HYC1"'"3%-CWO1QO
 G;3)O8C|?85>*¬3ΔKOC.IΔL+CRLXQ JXCOCUAMC1FOO3;¬ERO_K:¬)JJH(3
+<;&J5PO?4|&ENGC R;&
F52O?27IY;"9J_TNTU8O8WH&-LC9?CUFLR81ΔL3KΔJWOC4(&>¬OMR|337 11
A=TDAR557_A&1Z-1*KQF
HN¬KMAUID| 5C-F&1FD6%:5I_?J1K:6-C9D5M"5&21F1'CTI,  54I_LX.CK
+E;;5V;G/G7_JJOOZ>Y&
C Jv¬&XC%AHOZA/&-QOO8CC&,E.CLP &+OOC*T<&38=O CC&_5/OC6_&%V/O
FU%&2Y*OV=;& F406%V&
HVVAX3¬&A(Mw* >M?6 MSALRZ/T3OKG4 +=9+RNF5H?M*VLCOYΔ04QDJD 4M
?7Z)9UM5  NCOTOS_2&
O <BY(M&'45W_5.M31 ZO PGEGO3E 44'KX9N%SF%|?Z%%:CLΔ<M)J=&*H+L
AB¬&,J9W)L8G%VBB3( (
COXC& R&,2UN(S8MOFIV"U.2+H'7K L&w¬,K6MZ3||¬927%&9B|V2 *MMW:1
 > 9¬(MOVK:N5|H5 6Δ&
CZ>DA?>& E_O<RΔC>-64|A(FFZ2L7? DΔXJ8SΔE/DC¬V45CMT8R5.55J"O,L
9AA&3QQVMDPI)6&1OL8O
X%COJJL&K< 9COIMF P4 I22 CG97"+4I¬ZIC+D3Q*=WQQOZPKUL/K7D 1ΔW
O6B2:LBU,BLCF8.I (F&
"  O/NH&1'&9 >'R,=w1_).&4MO8I_(&2AOX|GRNTO=O3*HP  T3%=R R,5
QE*IQPSWMB:&|<ΔL9?S&
W(AOD&(&J/HKTDIP5G CH1"C%JO5M+EA *SK5/"NXBOZOAFJ ¬BX,1JRPL K
+ICIT(+1ΔR1&CC_CA1&&
F? EOWS&6(C8N(<S ¬3V=&WI6ZBOD)ON ,|L3;4CVG3&- ,JS"Q2O.*LYV25
G% GB.K981LM<6%O_5(&
V|"OE(G&*.>N+IY&/7¬L9¬|F%7SO|+?&B2VC6C9&O;EO+(Q&*;-O"| &3CQO
F"J&LO.OZC,&><COPV &
H.wOS Δ&=O 5&R3JJTX3YNRF<X13S;9N_NZLMNRF 8DO1FN&,;PO_+|&OCGO
=E;&_ 2OL -&CN:O*%7&
MY'O 2A& 8=Z7I6C,%8OF.2&C5OO| R&48TCBF3&  3ON2S&2|=O>%D&G5WO
KXO&SWIO(MV&KTIO2 U&
O)DOQZO&?*VH/Δ,UOI?C:24N%XO5D_WC%|L1R YDQ'OOD=:2O;&Z*'I38C5N
 1=1)OFZ*KQG 1<5N U&
TJOOGWO&&D.O"4 &COCCRXRFWR=O-3C&5W/CWZ_&TC/O,Y%&JN*O)U;&9R4O
XDV&F&GO>(¬&R77O|H>&
```

```
**********************************************
*         LISTAGEM IV - CRIPTOGRAMA          *
**********************************************
```

```
,CSCA%O&MF 5IwFED=_6NLJO<X>1-"UJ B=LHMC&& VO89ZF4FFM(* FFR6W
H?UI¬%(w"SV&NMwV-XZ(
/B9O(J5&/&CMERPRW<'C;,BN/G>OU4:NU:CwZ/VNA,<WEA62%XQLPC*R_1-O
2O 1B&E4,(:J.ATwZL9&
,' 09: & &'O7TYN-38LCU)&G,¬U/6"3O*FCDA).5*3T9(< >%JZ T+,DOU&T
>Q92>*IO>C?&3CU4-OOC
)27OZC?&WKVM4¬Y2P(A53.OI C+5<+KC.C)C9L/&J&'O(Y &6:QO1GK&<P&O
6=9&¬DCO_AL&C9LOOOB&
Y8AO/21JM_F55%;&QQ-CY ENZ,'XA DMVTXZOCNJ.CYO=X9N'MFXI ONPF'5
PLEF:R w"MJF%L3UV|¬&
C 5OH_Z&RCN5 R*&335U'4<CZT/K:?AD-D9CO')R7-S3 F.2Z)-4UQ_FYBCZ
,_WR9"TJZB(&CPAO¬ <&
3.AwS| N9FJUF1E2 CC96::&":PO XQPO%O1FCFE+*+5OW>JS9 WQC4IPZWO
XEH4 &MTESN%|FWQ3&J
"2wO&>T&NICO GK&A7+07 4&CZ6C*O,&G RC*:N&BARO9(M&A|MOY6F&RO%O
)_(&7P"O&CG&_K?O ;O&
NY O 7Q&B*SO%??&.3VC6;9&>VEC%BQ&_C-CYV &AWQO*GJ&?4.OUE,&B.CO
(A &+ WO HA&;?+O""3&
 21OGF)&>*1O1T*&&>%C6Z+&3|DC&;N&'GPC|Z|&¬2GO?1;&O=2O+|-&¬-:O
+_7&HI'O 4A&CT)O52-&
<H8O1B2&A8OC*2R&XJTCJ13&BH3OV>S&4U=C' D&=OWOT7O&+6IO<XV&>9IO
7>U&G DO.CC&.-*O2C)&
WD:6X KENG;TC9W&<1O%(w4<8C+%FCT<AXI%NBN<MBZ%R.4<)+<%Q2:&"FHO
MJ/&) OO:CO&:B.09& &
F3C6OUIE U"T)TC&MO'C(C_&ZK/O'%%&7A*C, ;&Y%4ON*V&V9GOFX¬&9W7O
L4>&K SOQ:O&P OVEG&
B¬86%RMEN*<T|?O&M84O/-CF+H/UOU?F¬A 1MC FD= 4=O1RUK>OP M&WXOO
AC.&TK9O_T5&LX907¬4&
7T/6;'IEL'(T.Z_&5ACC4DX&>:|OPU6&U :CU+8&"KBO=¬|&Z3EO<?R&PHVO
DA8&-9 O(& &/P8O5,1&
RF=6+?+E>T:T)?:&": %CC <X 2%H.|<_7(%&T/<9U(%IR-<IR&%+A>& 9UO
w 5& &7O¬6?&&IXOMG=&
QIKO66IEA )5-_3)3U69014L::< PB&AA|'6(|C 'E3<PI(WHC'POL&4QLO
K_B&M|;O1RU&_(FO7¬C&
5¬ZO(OAJJDZ9)CJL8CwJ-T.OXHACE_ OUV2CA| OQ-BCAZOO9UPC% 5O9(|C
N?S1;&50*|Z&.SNO:1H&
=&UOL= &LQYO(OA&OFCO 5C&.B,C ; &,"6CA"%&BO;O6CT&U?AOL4(&K+AO
G?<&*8AO:'=&G5MOLIE&
R_XO>M&N:=3ZC F¬KA1/ L3,9|K*U4OCCHLI)X2 I_X C4-XJO"L"O%%NM
"9(N,H2ZH+W2RYCO9DK&
Q<+O'9¬J//M3:BHF5+QK"4NG3C(5IYN&_(GM='U&K>9&*X?&9-AWEWKJI/(5
&+¬E:Y8O VQ&UGSOX|?&
?3VOO 9&M,EO76Q&FC-OWO &EHQO>&J&B%.CD&,&DICO&) &:4WOXFA&?I+O
J?3&*T1O29)&-L1OVY*&
```

****
* LISTAGEM IV - CRIPTOGRAMA *
****

```
OC%03|PN&WIAGFH&DDBNPC|&2/GC_);&?T2C%)-&% :0*_7&MZ'006A&& )0
6F-&:V80282&ACOOWCR&
JZTO7C5F,32LBW J%K7G*YD&L,WCKGO&KGIC&9V& &IOYKU&C7DOL6O&9K*O
(A)&* ?OLQP&C)¬06EW&
N6 O"Z:>5 KC<""&DANO"AI&SV5C..Y&,|&CPI:&WZHOW /&(BOOL:O&HA.O
"% && OO(;<&3H=06MC&
 G/O:(ZH=C//C GYT>*C+1;&C"4C 5V&ASGC,A¬&IM7OU->&/USOUHO&<V 0
 EG&2 _O<¬J&2A(O,CO&
?MYOP>.OEK_/)H%HV:+CI8-F_LTOOS2&IO>C<YM&L/UOKM.&AT9OK55&3=90
MC4&ZB4OL"W&>X<OOS_&
 E¬OB"O)2N11X/,&Y?:C;A8&O'BOX"|&N4EC8JR&V|VOFO8&*6 05W &Y:80
E41&Yi,OR5.&GZCOX.:&
=?FOOF+>>P¬05HL&)CJO:2'&;?JC- A&C1<C S>&G.UO/C5&>D709&?&W8XO
83=& OKO?C &"& C6_P&
S )OPPYO?|65P O(I3+LU3T-A*&CI|9&26CCO&L&A7LO5ZB&&T;O?7U&2HFO
3O&&U?ZOMBE&V&ZOKDC&
H'UO?R2FX)ICC C/G(|C357&6U"CB,F&AG CR-H&'¬2OH|¬&&*5042Z&(YNO
7VH&.(OOJM &::YO);A&
B"&A&"+B|N9=>WC-HYC9D))(ON;C;<T&F-ACBW(&?DAO)3<&<UAOXU=&NHMO
)/E&.UXOJ>"&:<PO:P+&
=7BO;&RO==?C7F%EFX(7¬CX&"¬)O2>&&7CHCKIS&8N OL/I&+U3O,CT&(FCO
  K&//+O9P4&;¬6CG*,&
:%RCW¬AN9Y OVN1ND=(CMXLLN OZO HRQ""37VUJAO85IO2IJ5<+4QRCS3-O
4¬¬-?">OES9& 2EOO Q&
VM-09J>F<¬QTCZ:B<V.OH ,&6HCC-9 &(ZWC EA&-U+OA-3&4M1OS,)&- 1O
F%*&_H%OE5+&>5DOE|N&
DQPOO)Q4-L TV4PG?)18( '&R5:CG_7&7 'C 9A&X1)OTC-& B8OH>2&O'OO
%CR&2BTO¬E3&JF3O,XS&
_+=O:GUS6)FS)CC&%QICR.V&MXICG6U&6CDCOAO&WE*OW4)& T?O*KP&8,¬O
SJW&FU O/PY&N5KOC¬"&
BANO:TI&<%5O""Y&*<&C"¬:&(<HO4S/&5OOCJCO&F .OLH &Q+OO**<&CT=O
_DC&P8/O,"_&T /OZ5%&
PC*OEPIJX31ON.U5¬LG37|ILF 7W-(_J| 45GPVJ/O XH*A4S.ZW/-JMQT+1
_OWN3<YOSCB&GC-OV5Z&
<&LOAQM4_5,O=5"G>S3C 8VO2>.CI3?E?9O_PA./ FUO;X4&W+4OGFW&. <O
; _&6(¬049X&GP|OIA6&
K4:O8 =FR3CL_K8S";'1N>R&BNVO5U8&¬3 C3' &?*8OLA1&>A,O&".&&XOO
'X:&VUFO?D*&*J>O38L&
-<JO%UY5GC4&W+A&9;<C7H>&D;UOQC5&I%7C8 ?&-XXO -=&|:KO)K &OC O
&_P&&O)O/ /&/D'O3V &
)&QO2ZUF.Y&V|IHO CO/:L&3NLOVVB&48;CSCU&OCFO( C&Z ZO¬ME&X2ZO
GZD&W UOP¬6&4;AOZ&'&
6Y|O|?=JHC"CN7F&V) OO+H&N 2OE?¬&R)5CKMZ&;?NO/RH&¬ OOT  &-)YO
 WA&V8COC G&F",O1P &
```

****
* LISTAGEM IV - CRIPTOGRAMA *
****

```
VZ6O-OYFLH;/)(HB=&AO6R(& CAC-7<&CJACZ =&/CMOT9E&4"XO I"&?OPO
=C+&X*BO9;&&C5 O/VX&
YC(O?SU)C.LUXF)EA.9 MT3(6Q C7II&Y'3C&_T&OVCOLAK&|5+OZ54&RR6O
H%,&MARQL1N&W RCL:M&
X5MOOI|O*F/AE)QN2BSOC-UF3|¬OOBO&>6 CIBQ&D)SO3|?&35VOMD9&+9EO
N;Q&<J-O/Y &K+QOI-J&
(;.O2U?FC=C/ X1BG;WCACA&?"+C(&3&SD1CQ)).&OA1OMO*&W4%O_*+& HDO
 XN&OAPOC7|&W=GO|6;&
+_2OH9ZCZN7/KWSNC&-7AQP&7Q)O=?-&/¬8C2U2&: OOO,R&ICTO)?3&-V3O
STS&US=OYVD&C-WOEYC&
)ZIOX)%JT7H=SCU&Q&DOSBD&K8*CO%)&?%?C.(P&?:¬O*)W&)" O8EY&'¬KO
G""&U'NOCEI&D25O¬3Y&
MH&OD59FW<AVC?/&M4OC4|C&2".O3V &ACOC/C<&S'=OA4C&OZ/OS2_&O6/O
B9%&KH*OK';&?L4O(VV&
(3GOA6QFPU:B)K)-R KC>NCWU&) 1_+J ,_CYTJ&QI(O %O&:+YOB B&ER-O
H)Z&SZLOQBC&3MIOS 2&
U >G;U)L5BPJSLP<EE9C, 5&=,9CN<4&ZC4C=<W&X(<OSK_&IO¬O<3X& W|O
6H6&T8:O2R8&CKBOJ |&
35cONU&OTNWOPO3Z4CGWWE /D|8C;D1& :,C%I.&HWOO/D:&3QFO&B*&C%>O
+YL&9'JOLO'&'*JOAKA&
5.<OY?94 2ZS%EY>KBLV;<SR QO_Y<=&F¬KC / &OV OF>P&OC)OT*/&>,'O
D9 &8_QOH-K&HS&OJ¬9&
SXCHSVL&Q4 4*5MM3 .1 EM<D.CC5-F&FJZC?XE&8IZOZ(D&.OUOLV6&"JAO
)H'&7O|O& 7&VA"C6DF&
OS OGA¬4R6"S VB>C JV7=UR:8U_8+H&CGOC. &F YO4>A& OCO,MG&I=,O
Q3 &*)6O¬:%& .;OE%T&
+AAE¬.(&N2H5>? M<3Z1/A+<O ICO/Q&MXXCHT"&MZPO&?+&7 BOI%&&R O
?WX&KA(O,L1&B'_O;O&&
IAHOK554WR(S9EM>OBPVR¬>RD 2_48K&T +C|L4&4M6OWA,&G(RODCN&:PRO
/;M&>BMO2|F&<F%OA+(&
X:"DUOG&=(W7MC M"6|1ZAY<¬4"C4 2&Q6VCYX9&S EOXLQ&9+-O;= &P1QO
KYJ&EP.O >,&WFCCY2 &
YLWO)A,4.RCSP3>>>SNVJG&RI9 _|4*&W/%CZB+&V DO_"N&Y PO(K|&G_GO
4S;&7J2OFH-&|.:O5>7&
A<'C='A&C=M88P6M_6_1L B- YA %LR&Q4TC 3&)C3OW¬S&B7=O.CD&+CWO
 8U&V91O9CV&6MIC."U&
A)LOZIA4YYJS>C >ES.V)| R;G>_S W&*D CD3Y&C KO&-"&A=NO XI&.95O
_YY&ME&O|.:&QJHOG2/&
Z_OB<ROE('B/;NAM 5C1CYA(SZ+_1UC&6R/C)U_&Q_/OH'%&L4*O4T;&R74O
?'V&H*GOA&¬&&/7OWV>&
6LSOE3X43FXSI7 >QCIV)>*RC=A_( O& ,YC7&B&B*-OYEZ&?BLON%C&*3TO
IU2&<M>O+CM&NKCO D.&
&N9A?%S4|A4SV+'G&'78GG,/*1'_U _&L¬¬CI_X&*5|OON6&C':O<G8&='BO
J-|&U6EO<8R&ZTVOR(8&
```

****
* LISTAGEM IV - CRIPTOGRAMA *
****

```
9% O_Z &9S8CV<1&)3,O_M.&?VCCK-:&Y(FCX *&9G>OFQL& >JO/H'&TLJO
(OA&98<O?^>&:DUO=.5&
T=7Ow¬844G?CBL3G>(|CJJ1CBBGCP93E11M_AP¬/- -OC( &  QO2OK&EU&O
&G9&% COY|L&_LLO_;B&
3S;OYKU&:8FCP-C&9SZCE9E&Q-ZO81D&8TUCV%6& DÆO+ '&>9|O6U7&B&"O
T&F&SW O>,H&S¬2OPC¬&
O;5O,Q F9;*VCGH&;COCHP & TYC:7A&JZCCV;C&Æ',O<| &OK6OL8%&¬W;O
E*T&42AO_'(&¬ZAO_ <&
C,ÆO%O=&7 MCX E& &XC '"&YCPC?C+&>VBC|:&&C. O WX&M*(OCX1&3T_O
7 &&)RHO2,S&C) O7 I&
A>B 9AEI. F'K;T-?B+C 24&>|6C/<,&&;RCCNN&;_ROCBM&Æ+MOHNF&F9%O
*G(&(C"O5,G&7*?O CC&
; , (;;FSWTLS/HOY7W1C¬)CLSE4TS)&W E5YM'NHEQU)UG24,¬0782JXX;Z
¬|IUOETLXÆ &%4+C'C3&
CW1OJ; JS?1K2-*GYP MSZ FMO-C5RND<C5C_:|H2RGWWC:DC/7Z%¬CR*C:4
2>4J1|,5 B*&CV)OOP-&
VQ8OGJ&3VJOC>ÆR&;<TCHD3&IS3C7*S&G<=CT/D&¬DWO%HO&D IOJBV&),IO
1TO&C DOE|C&X)*O)))&
¬'?OPAKE?Q¬C66W&AI OESY&Z5KC6 "&D"NC  I&S 5OX*Y& B&O6S:&Æ4HO
(O/&6VOOYTC&PÆ.OC) &
V1 %N.&<K?=5)6F&( 7CG¬9&_2/5GG8G|7*4? )I )P1HL1&"EC5S3OG8+05
"J2<Æ,=%9)%<C<6%; C<
```

```
*****************************************
* LISTAGEM V-MENSAGEM ORIGINAL RECUPERADA *
*****************************************



C      ****                    ******

C      * CONJUNTO DE CARTOES TESTES *

C      ****                    ******

C

       SUPONHAMOS QUE ESTE SEJA UM PROGRAMA DE GRANDE VALOR E
 ESTRITAMENTE CONFI-
DENCIAL.ESTE METODO DE CRIPTOGRAFIA UTILIZA TECNICAS CLASSIC
AS.
       PRIMEIRAMENTE FOI DEFINIDO O ALFABETO COM O QUAL TRABA
LHAMOS.ESTE ALFABETO
E OS CARACTERES DO FORTRAN(A-Z,0-9,E OS CARACTERES ESPECIAIS
 $/+-*.,()='& E O
BRANCO).

OBS1     METODO DE SUBSTITUICAO UTILIZADO= SUBST.COM ALFAB.MU
LT (VIGENERE)
OBS2     METODO DE TRANSPOSICAO UTILIZADO= TRANP.COLUNAR (MAT
RIZ 80COLS POR 20LN)
OBS3     CHAVE1 DEFINE AS REGRAS DA SUBSTITUICAO (LINHA DA MA
TRIZ DE VIGENERE).
OBS4     FOI UTILIZADO SOMENTE UMA CHAVE1 ,ENTRADA DE UMA ROT
INA DE NUMEROS ALEA-
         TORIOS.DIVIDIMOS TAIS NUMS ALEATS.POR 49 E TOMAMOS O
 RESTO(MODULO 49).
         ASSIM SIMULAMOS A CHAVE DO PROCESSO ORIGINAL (VIG) E
 TORNAMOS O SISTEMA
         MAIS SEGURO.O ALFABETO JA ESTA EMBARALHADO P/MAIOR S
EGURANCA
OBS5     A CHAVE2 E NUMERICA.PODERIAMOS FAZE-LA ALFABETICA ,E
XEMPLIFICANDO=
         CHAVE2=  METROPOLE

         NUMERO ASSOCIADO A CHAVE METROPOLE

         METROPOLE

         319857642   NOTE QUE A LETRA O MAIS A ESQUERDA TEM V
ALOR CORRESPONDENTE
                     MENOR.
```

```
*****************************************
* LISTAGEM V-MENSAGEM ORIGINAL RECUPERADA *
*****************************************



      NO ENTANTO FOI FEITA UMA ROTINA QUE LE OS NUMEROS NO
 FORMATO I1 (80NUMS)
      E SUBSTITUI AQUELES REPETIDOS,BEM COMO SUBSTITUI OS
 ZEROS DE TAL FORMA
      QUE O RESULTADO E UM VETOR  CHAVE2(I),I=1,80 COM VAL
ORES DE 1 A 80 DIST-
      RIBUIDOS ALEATORIAMENTE.

OBS.FINAL= ESTE FOI UM EXEMPLO DE CRIPTAGEM E DECRIPTAGEM BE
M COMO O PROGRAMA
         E UM EXEMPLO.COISAS MAIS SOFISTICADAS PODERAO SER
 FEITAS.
  O QUE VEM A SEGUIR E UM  PROGRAMA CONFIDENCIAL (OU ERA...
) QUALQUER EM FORTRA
  N

*

*

*

CONFIDENCIAL      ************************************

CONFIDENCIAL      *                                  *

CONFIDENCIAL      *  PROGRAMA FORTRAN CONFIDENCIAL   *

CONFIDENCIAL      *                                  *

CONFIDENCIAL      ************************************

      INTEGER A(8),IPUNCH(10),B  ,P(10),PUNC(10),N (8)

      DATA IPUNCH,B/'0','1','2','3','4','5','6','7','8','9',
' '/
C

C     LEITURA DOS CARACTERES ALFABETICOS A PERFURAR (A),N=NU
M DE CARTOES
C     ,A-ESCRITO NAS 8 PRIMEIRA COLUNAS E N-NAS 8 COLUNAS SE
GUINTES
C
```

```
      ******************************************
      * LISTAGEM V-MENSAGEM ORIGINAL RECUPERADA *
      ******************************************


        READ(1,1) A,NV
      1 FORMAT (8A1,I7)
        K=8
        DO 2 J=1,8
        IF(A(J).EQ.B) GOTO 3
        P(J)=A(J)
      2 K=K-1
      3 IF(K.EQ.0) GOTO 100
        DO 15 IK=1,K
     15 NK=NK+9*10**(IK-1)
        IF(NV.GT.NK) GOTO 100
C       ZERAR O VETOR PUNC -PRIMEIRO CARTAO PERFURADO=..ALFAB.
.000...
        DO 4 L=1,K
      4 PUNC(L)=IPUNCH(1)
        K2=8-K
C
        PAUSE 'FAVOR COLOCAR OS CARTOES NA   PERFURADORA DE CA
RTOES'
        PUNCH 6,(P(I),I=1,K2),(PUNC(I),I=1,K)
      6 FORMAT (72X,8A1)
        NV=NV-1
        DO 7 NA=1,NV
        IA=0
```

```
      ********************************************
      * LISTAGEM V-MENSAGEM ORIGINAL RECUPERADA *
      ********************************************


      DO 8 J=1,K
    8 N(J)=MOD(NA,10**J)
      IF(N(1).NE.0) GOTO 10
      DO 9 J=1,K
      IF(N(J).NE.0)GOTO 9
      IA=IA+1
    9 CONTINUE
      GOTO(20,30,40,50,60,70),IA
   70 IC=NA/10**6
      IF(IC.GT.9) GOTO 100
      PUNC(K-6)=IPUNCH(IC+1)
   60      ID=MOD((NA/10**5),10)
      PUNC(K-5)=IPUNCH(ID+1)
   50      IE=MOD((NA/10**4),10)
      PUNC(K-4)=IPUNCH(IE+1)
   40      IG=MOD((NA/10**3),10)
      PUNC(K-3)=IPUNCH(IG+1)
   30      IH=MOD((NA/100),10)
      PUNC(K-2)=IPUNCH(IH+1)
   20      IJ=MOD((NA/10),10)
      PUNC(K-1)=IPUNCH(IJ+1)
   10 PUNC(K)=IPUNCH(N(1)+1)
```

```
*********************************************
* LISTAGEM V-MENSAGEM ORIGINAL RECUPERADA *
*********************************************
```

```
C

      PUNCH 6,(P(I),I=1,K2),(PUNC(I),I=1,K)

C

    7 CONTINUE

C

  100 WRITE(3,101)

  101 FORMAT(1X,'ACABOU,OU DEVE HAVER PELO MENOS UM CARACTER
 ALFABETICO
     *PARA SER PERFURADO,OU HA MAIS DO QUE O NUM.PERMITIDO D
E CARTOES')
      STOP

      END

********** ESTE E O FIM DO EXEMPLO DE CRIPTAGEM E DECRIPTAGE
M ******************
```

3 - Frequência das Letras em Textos Escritos: (Lingua inglesa)

Ordem e frequência das letras

E	1231	L	403	B	162
T	959	D	365	G	161
A	805	C	320	V	93
O	794	U	310	K	52
N	719	P	229	Q	20
I	718	F	228	X	20
S	659	M	225	J	10
R	603	W	203	Z	9
H	514	Y	188		

Ordem e frequência de aparecimento dos diagramas.

TH	315	TO	111	SA	75	MA	56
HE	251	NT	110	HI	72	TA	56
AN	172	ED	107	LE	72	CE	55
IN	169	IS	106	SO	71	IC	55
ER	154	AR	101	AS	67	LL	55
RE	148	OU	96	NO	65	NA	54
ES	145	TE	94	NE	64	RO	54
ON	145	OF	94	EC	64	OT	53
EA	131	IT	88	IO	63	TT	53
TI	128	HA	84	RT	63	VE	53
AT	124	SE	84	CO	59	NS	51
ST	121	ET	80	BE	58	UR	49
EN	120	AL	77	DI	57	ME	48

Ordem e frequência de aparecimento dos diagramas.

ND	118	RI	77	LI	57	WH	48
OR	113	NG	75	RA	57	LY	47

Percentagem dos grupos.

A E I O U	38.58%
L N R S T	33.43%
J K Q X Z	1.11%
E T A O N	45.08%
E T A O N I S R H	70.02%

Lista das inversões mais comuns.

ER	RE	ON	NO	TE	ET	ST	TS
ES	SE	I N	NI	OR	RO	I S	SI
AN	NA	EN	NE	TO	OT	ED	DE
TI	IT	AT	TA	AR	RA	OF	FO

Ordem de aparecimento dos triagramas em 10.000 letras de um texto semi-militar.

THE	ENT	FOR	NCE	OFT
AND	ION	NDE	EDT	STH
THA	TIO	HAS	TIS	MEN

Tabela comparativa de frequência de letras (%)

INGLÊS		ALEMÃO		FRANCÊS		ITALIANO		ESPANHOL		PORTUGUÊS	
A	7.81	A	5.	A	9.42	A	11.74	A	12.69	A	13.5
B	1.28	B	2.5	B	1.02	B	.92	B	1.41	B	.5
C	2.93	C	1.5	C	2.64	C	4.50	C	3.93	C	3.5
D	4.11	D	5.	D	3.38	D	3.73	D	5.58	D	5.
E	13.05	E	18.5	E	15.87	E	11.79	E	13.15	E	13.
F	2.88	F	1.5	F	.95	F	.95	F	.46	F	1.
G	1.39	G	4.	G	1.04	G	1.64	G	1.12	G	1.
H	5.85	H	4.	H	.77	H	1.54	H	1.24	H	1.
I	6.77	I	8.	I	8.41	I	11.28	I	6.25	I	6.
J	.23	J	...	J	.89	J	...	J	.56	J	.5
K	.42	K	1.	K	...	K	...	K	...	K	...
L	3.60	L	3.	L	5.34	L	6.51	L	5.94	L	3.5
M	2.62	M	2.5	M	3.24	M	2.51	M	2.65	M	4.5
N	7.28	N	11.5	N	7.15	N	6.88	N	6.95	N	5.5
O	8.21	O	3.5	O	5.14	O	9.83	O	9.49	O	11.5
P	2.15	P	.5	P	2.86	P	3.05	P	2.43	P	3.
Q	.14	Q	...	Q	1.06	Q	.61	Q	1.16	Q	1.5
R	6.64	R	7.	R	6.46	R	6.37	R	6.25	R	7.5
S	6.46	S	7.	S	7.90	S	4.98	S	7.60	S	7.5
T	9.02	T	5.	T	7.26	T	5.62	T	3.91	T	4.5
U	2.77	U	5.	U	6.24	U	3.01	U	4.63	U	4.
V	1.00	V	1.	V	2.15	V	2.10	V	1.07	V	1.5
W	1.49	W	1.5	W	...	W	...	W	...	W	...
X	.30	X	...	X	.30	X	...	X	.13	X	.2
Y	1.51	Y	...	Y	.24	Y	...	Y	1.06	Y	...
Z	.09	Z	1.5	Z	.32	Z	.49	Z	.35	Z	.3

Percentagens de vogais

Inglês	Alemão	Francês	Italiano	Espanhol	Português
40%	40%	45%	48%	47%	48%

Percentagem para L N R S T:

33%	34%	34%	30%	31%	29%

Frequência de DIAGRAMAS da língua inglesa (p/10.000 letras de texto literário).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
A	1	8	44	45	131	21	11	84	18			34	56	54	9	21		57	75	56	18	15	32	3	11		805
B	32			18	11	2	2	1	7			7	9	7	18	1		4	13	14	5				11		162
C	39		12	4	64	9	1	2	55			8	1	31	18			14	21	6	17		3	5	10		320
D	15			10	107	1	1	1	16			28	2	118	16			16	6	9	11		4		4		365
E		58	55	39	39	25	32	251	37	2	28	72	48	64	3	40		148	84	94	115	53	30	1	12	5	1231
F	10		1	12	23	14	3	2	27			5		8	94			6	13	5	1		1		3		228
G	18			2	20	1	1		10			1		75	3			6	6	1	12				5		161
H			46	3	15	6	16	5					1	9	3	7		3	30	315	2		48		5		514
I	16	6	15	57	40	21	10	72			8	57	26	37	13	8		77	42	128	5	19	37	4	18	2	718
J		2		1	1	1						1		3				1									10
K	10		8		2				8			3		3	5			11	2								52
L	77	21	16	7	46	10	4	3	39			55		10	17	29		12	6	12	28		4		6	1	403
M	18	1		9	43	3	1	1	32			4	5	7	44			15	14	14	9		1		4		225
N	172			5	120	2	3	2	169		3	1	3	9	145			12	19	8	33		10		3		719
O	2	11	59	37	46	38	23	46	63	4	3	28	28	65	23	28		54	71	111	2	6	17	1	28		794
P	31		1	7	32	3	1	1	3			2	16	7	29	26		8	24	8	17		2	4	7		229
Q	1			1	14							2							2								20
R	101	6	7	10	154	4	21	8	21			2		5	113	42		18	6	30	49		1		5		603
S	67	5	1	32	145	8	7	3	106		2	12	6	51	37	3		39	41	32	42		3		17		659
T	124		38	39	80	42	13	22	88		1	19	6	110	53	14		63	121	53	45		6	1	21		959
U	12	25	16	8	7	11	8	2		4		8	13	12	96	7	20	6	30	22			1	1	1		310
V	24			4	16	1			14			2		4	13			5	2	4			1		3		93
W	7		1	9	41	4	2	7	1		3	5	2	15	36	1		10	27	16			2		14		203
X					17				1					1							1						20
Y	27	19		6	17	1	1	1			3	47	3	14	4	2		17	4	21	1						188
Z	1								4						2						1					1	9
																											10000

Frequência de letras como letras iniciais de um texto de jornal c/16 410 palavras arranjado alfabeticamente e pela frequência.

A	1802	T	2614
B	757	A	1802
C	918	S	1213
D	459	O	1176
E	410	I	922
F	666	C	918
G	293	W	833
H	636	P	768
I	922	B	757
J	95	F	666
K	88	H	636
L	348	M	578
M	578	R	513
N	401	D	459
O	1176	E	410
P	768	N	401
Q	31	L	348
R	513	G	293
S	1213	U	224
T	2614	Y	126
U	224	V	100
V	100	J	95
W	833	K	88
X	10	Q	31
Y	126	X	10
Z	6	Z	6

Frequência de letras como letras finais do mesmo texto.

A	480	E	3325
B	25	S	2077
C	107	D	1649
D	1649	N	1592
E	3325	T	1587
F	744	R	906
G	463	Y	903
H	407	O	745
I	72	F	744
J	6	L	599
K	148	A	480
L	599	G	463
M	220	H	407
N	1592	M	220
O	745	W	166
P	84	K	148
Q	1	C	107
R	906	P	84
S	2077	I	72
T	1587	X	34
U	29	U	29
V	15	B	25
W	166	V	15
X	34	J	6
Y	903	Z	5
Z	5	Q	1

As palavras mais comuns da língua inglesa.
Contagem feita em 242, 432 palavras de textos de quinze autores diferentes. (Textos jornalísticos).

THE	15568	OR	1101	WHEN	603	ONLY	309
OF	9767	HER	1093	WHAT	570	ANY	302
AND	7638	HAD	1062	YOUR	533	THEN	298
TO	5739	AT	1053	MORE	523	ABOUT	294
A	5074	FROM	1039	WOULD	516	THOSE	288
IN	4312	THIS	1021	THEM	498	CAN	285
THAT	3017	MY	963	SOME	478	MADE	284
IS	2509	THEY	959	THAN	445	WELL	283
I	2292	ALL	881	MAY	441	OLD	282
IT	2255	THEIR	824	UPON	430	MUST	280
FOR	1869	AN	789	ITS	425	US	279
AS	1853	SHE	775	OUT	387	SAID	276
WITH	1849	HAS	753	INTO	387	TIME	273
WAS	1761	WERE	752	OUR	386	EVEN	272
HIS	1732	ME	745	THESE	385	NEW	265
HE	1727	BEEN	720	MAN	383	COULD	264
BE	1535	HIM	708	UP	369	VERY	259
NOT	1496	ONE	700	DO	360	MUCH	252
BY	1392	SO	696	LIKE	354	OWN	251
BUT	1379	IF	684	SHALL	351	MOST	251
HAVE	1344	WILL	680	GREAT	340	MIGHT	250
YOU	1336	THERE	668	NOW	331	FIRST	249
WHICH	1291	WHO	664	SUCH	328	AFTER	247
ARE	1222	NO	658	SHOULD	327	YET	247
ON	1155	WE	638	OTHER	320	TWO	244

BIBLIOGRAFIA ANOTADA

1 - Allen, Brandt: "Danger Ahead !
Safeguard your computer"
Havard Business Riview -
Nov - Dec 1968

Este é um dos melhores artigos disponíveis sobre problemas gerais de segurança de computadores.

2 - Beardsley, Charles W.: "Is your
computer insecure?"
IEEE SPECTRUM - Jan. 72

Segurança em geral também é a tônica do autor.

Na área de "criptografia" apresenta um interessante quadro comparativo dos métodos ou técnicas de "criptografia", Vernam (método 1), Vernam (método 2), Vigenère.

No quadro comparativo são considerados:
o tamanho da chave; memória adicional requerida, dificuldade de decifragem e custo por bit para codificar e decodificar.

3 - Chesson, Frederick W.: "Computers
and Cryptology"
Datamation - Jan 73

Um exemplo de programa de criptagem em linguagem Fortran. Uma análise de criptagem e decriptagem é feita.

4 - Comber, Edward V.: "Management
of confidential Information"
Proceedings of Fall Joint Comp.Conf. - 1969

Segredo de informação é o tópico, mas também discorre sobre contrôle de segredo por computador.

5 - Consideration of the Application of
Criptographic Techniques to
Data Processing.
Fall Joint Computer Conference
AFIPS - 69 number 35

Duas técnicas de criptografia são descritas. Um método é o de substituição digital, análogo ao Vernam, usando uma combinação controlada de dados e o conteúdo de duas memórias. O outro método usa uma transposição digital de matriz, fazendo uso de uma combinação de transposição de linha e coluna sob o contrôle de uma memória.

Possíveis caminhos para se alcançar a chave de cada processo de codificação são descritas.

6 - Graham, Robert M.: "Protection
in an Information Processing
Utility"
Communications ACM - May 1968

É sobre uma solução para o problema de acesso usando "anel" de proteção.

Esta combinação de hardware e software ajuda o contrôle de acesso para compartilhar dados e "procedures".

7 - Hammer, Carl: "Signature Simulation
and Certain Cryptographic Codes"
Communications of the ACM
Vol.14 uma Ser. 1 - Jan. 71

Um interessante relato do trabalho feito por decriptadores sobre um criptograma escrito em 1822. Métodos computacionais de decriptagem são relatados.

8 - Hoffman, Lance J.: "Computadores e Segurança: um Relatório"

Uma tradução do original americano feito na COPPE.

9 - Hoffman, Lance J.: "Computers and Security"
Journal of the ACM - Vol 1, number 2,
June - 1969

O assunto, um relatório, trata da segurança e de controle de acesso em sistemas de computadores. Faz ainda uma explanação breve sobre os aspectos legais e administrativos da segurança e controle de arquivos tidos como secretos ou de acesso unicamente a um grupo autorizado. Os métodos técnicos propostos até aquela data (de publicação do artigo) para controle de acesso são abordados, bem como as críticas êsses métodos. No que se refere à "cryptanalysis" o artigo cita brevemente no tópico "Transformação de segurança".

10 - IBM Research Reports
Vol. 7 number 4 - 71

As técnicas de "criptologia" são implementadas (transposição e substituição) por "hardware" no projeto intitulado "Lucifer", especialmente construído para tal finalidade.

Métodos de Vigenère-Vernam (métodos de "cifragem") estudados por Bryant Tuckerman, são mostrados, bem como a decifragem de mensagens, por meio da descoberta da "chave" que rege a mensagem.

11 - Krishnamurthy, E.V.: "Computer
Cryptographic techniques for
processing and storage of
confidential information".
International Journal of Control -
Nov. 1970

Exame de técnicas criptográficas em geral.

12 - Khan, David: "Codebreakers"
Macmillan Company, N.Y. - 72

A história secreta de códigos e transformaçoes secretas, desde épocas remotas até as mais recentes mensagens interestelares.

Apresenta um relato principalmente das técnicas usadas na segunda guerra mundial.

13 - Lickson, Charles P.: "Privacy and
the Computer Age"
IEEE SPECTRUM - October 68

O segredo e o computador são vistos sob o aspécto le - gal e jurídico.

Leis dos E.E.U.U. sobre o assunto são referidos.Previ_ soes futuras também são comentadas.

14 - Peters, Berward: "Security Consideratons
in a Multi-programmed Computer System"
Proceedings Spring Joint Computer
Conference - 1967

Descreve a proteção em um sistema de computação com acesso a distância multi-programado (multi-programmed). Sendo um

dos primeiros artigos, é um dos mais procurados.

15 - Petersen, H.E. and Turn: "System implications of information privacy"
The Spring J.C. Conference - 1967

Este artigo discute aspectos técnicos da segurança e segredo para sistemas computacionais.

Foi anexado em vários outros artigos e é um dos que valem ser lidos.

16 - "Security Controls in the ADEPT-50 Time-Sharing System"
Proceedings Fall J.C. Conference - 1969

Um sistema de segurança de Time-Sharing para o sistema IBM 360/50 é descrito com algum detalhe.

17 - "Security, Justice, & the Computer"
Paul M.Whesenand and G.M.Medak
Datamation - June 15 - 1971

Uma investigação dentro da condição de automatização de Sistemas de informação da Justice Criminal.

18 - Sinkov, Abraham: "Elementary Cryptanalysis"
Random House -

Os métodos criptográficos clássicos são vistos sob aspecto matemático.

A enfase é exatamente sobre características matemáticas da criptografia.

Abrange quase a totalidade dos métodos clássicos.

19 - Shannon, C.E.: "Communication
Theory of Secrecy Systems"
Bell System Technology Journal
Number 28 - 1949

Shannon desenvolve a teoria matemática dos sistemas secretos, discute no nível de obtenção de segurança, e liste as qualidades desejáveis para sistemas secretos.

É um artigo de tratamento matemático, muito bom.

20 - Tassel, Dennis Van: "Cryptographic
Techniques for Computers."
Spring J.C. Conference
AFIPS - 1969

Descrição de algumas técnicas clássicas decriptografia.

21 - Tassel, Dennis Van.: "Computer Security
Management"
Prentice-Hall, Inc. - 1972

Trata da segurança de computadores, desde a proteção das informações até a proteção do sistema global, instalações do computador, pessoal, etc.

Métodos de transposição, substituição, técnicas avançadas em "criptografia" são abordados.

Vasta bibliografia anotada está contida no final do livro.

22 - Theiss, Harold: "Commwnocation
Fheory ant Czberwetiks"
IEEE Student Journal - May 1965

Uma breve explicação da teoria de comunicação, modelos de sistemas e comunicação.

23 - Ware, Willes H.: "Security and
Privacy in Computer Systems"
Proceedings Spring Joint Computer
Conference - 1967

É um breve tratamento da configuração do sistema de time-sharing e identifica as maiores vulnerabilidades de penetração e saída de informações.

24 - Ware, Willes H.: "Security and
Privacy: Similarities and
differences"
The Saring, J.C.Conference - 1967

Uma boa discussão de segredo e segurança, diferenças e semelhanças.

25 - Wasserman, Joseph J.: "Plugging the
Leaks in Computer Security"
Havard Business Review
September-October - 1969

Segurança em geral é o tópico do artigo.

Apresenta um interessante "algoritmo" de teste de controle do sistema computacional.

Orientado para executivos e gerentes.